Unit E3

Homomorphisms

Introduction

In this unit you will study mappings whose domains and codomains are groups, and that (in a sense that you will learn about) preserve some of the structure of their domain groups. Such mappings are called *homomorphisms*. A homomorphism can provide insight into the relationship between the groups that are its domain and codomain.

You have already met many examples of homomorphisms in this module, because every isomorphism is a homomorphism – one that preserves *all* the structure of the domain group.

You will study some properties common to all homomorphisms, and meet the ideas of the *image* and *kernel* of a homomorphism, which are similar to the *image set* and *kernel* of a linear transformation (you met these ideas in Book C *Linear algebra*). The final section of the unit introduces you to one of the most important theorems in the group theory units: the *First Isomorphism Theorem*. This theorem brings together the idea of homomorphisms with many other concepts in group theory that you have already met – in particular, normal subgroups and quotient groups.

1 Isomorphisms and homomorphisms

In this section you will start by looking again at *isomorphisms*, concentrating on features that will be important in this unit. You will go on to learn what a homomorphism is, meet some examples of homomorphisms and study some of their properties.

For clarity, throughout this section and throughout the rest of this unit we will mostly *not* use concise multiplicative notation for abstract groups – instead we will use symbols for their binary operations. This is because we will usually be dealing with two groups at the same time – a domain group and a codomain group of a mapping – each with its own binary operation.

1.1 Isomorphisms

You met the ideas of *isomorphic groups* and *isomorphisms* in Unit B2 *Subgroups and isomorphisms*, and revised them briefly in Unit E1 *Cosets and normal subgroups*. You saw that two groups are *isomorphic* if they have identical structures – that is, if one of the groups can be obtained from the other by 'renaming' the elements (and the binary operation). A mapping from one of the groups to the other that carries out such a renaming of the elements is called an *isomorphism*. Remember that 'mapping' is just another name for 'function': it is often the preferred term in group theory and other algebraic areas of mathematics.

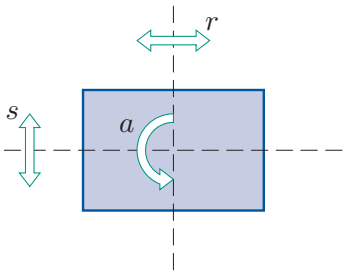

Figure 1 $S(\square)$

Until now our main interest when dealing with isomorphisms has been in whether or not two groups are isomorphic, but in this subsection our primary interest is in the isomorphisms themselves. We will start with another brief revision of the ideas of isomorphic groups and isomorphisms from this perspective.

Consider the two groups

- $(S(\square), \circ)$, the group of symmetries of the rectangle (see Figure 1)
- $(U_8, \times_8)$, the group of integers in $\mathbb{Z}_8$ coprime to 8 under multiplication modulo 8.

Their group tables are as follows.

$\circ$	e	a	r	s
e	e	a	r	s
a	a	e	s	r
r	r	s	e	a
s	s	r	a	e

$(S(\square), \circ)$

$\times_8$	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

$(U_8, \times_8)$

If we replace each entry in the group table of $(S(\square), \circ)$ by its image under the mapping

$$\begin{aligned} \phi : (S(\square), \circ) &\longrightarrow (U_8, \times_8) \\ e &\longmapsto 1 \\ a &\longmapsto 3 \\ r &\longmapsto 5 \\ s &\longmapsto 7 \end{aligned}$$

(and replace the symbol $\circ$ at the top left by $\times_8$), then we obtain the group table of $(U_8, \times_8)$.

Since the mapping ϕ transforms the group table of $(S(\square), \circ)$ into a group table for $(U_8, \times_8)$, it is an isomorphism and the two groups are isomorphic.

Notice that the first line of the specification for the mapping ϕ above is given as

$$\phi : (S(\square), \circ) \longrightarrow (U_8, \times_8)$$

rather than just

$$\phi : S(\square) \longrightarrow U_8.$$

When we discuss mappings between groups we often include the binary operations in this way, for clarity. However, as always, we can omit them if they are clear from the context.

There is usually more than one isomorphism between two isomorphic groups. For example, consider the mapping

$$\begin{aligned}\phi_1 : (S(\square), \circ) &\longrightarrow (U_8, \times_8)\\ e &\longmapsto 1\\ a &\longmapsto 5\\ r &\longmapsto 7\\ s &\longmapsto 3.\end{aligned}$$

If we replace each entry in the group table of $(S(\square), \circ)$ above by its image under ϕ_1, then we obtain the following table.

	1	5	7	3
1	1	5	7	3
5	5	1	3	7
7	7	3	1	5
3	3	7	5	1

Although this is not the group table of $(U_8, \times_8)$ that was given above, it is *a* group table of $(U_8, \times_8)$. The entries in the borders of the table are in a different order, but the entries in the body of the table have been rearranged accordingly. Thus ϕ_1 is also an isomorphism from $(S(\square), \circ)$ to $(U_8, \times_8)$.

An isomorphism from one group to another must be a one-to-one and onto mapping, of course – that is, it must match up each element of one group with exactly one element of the other group and vice versa, as illustrated in Figure 2.

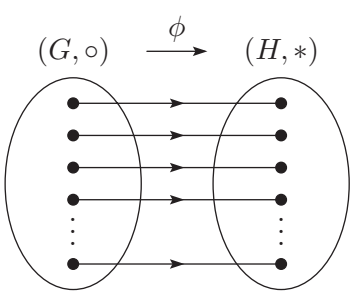

Figure 2 A one-to-one and onto mapping between two groups

However, even if two groups are isomorphic, not every one-to-one and onto mapping from one of the groups to the other group is an isomorphism. For example, consider the mapping

$$\begin{aligned}\phi_2 : (S(\square), \circ) &\longrightarrow (U_8, \times_8)\\ e &\longmapsto 3\\ a &\longmapsto 1\\ r &\longmapsto 5\\ s &\longmapsto 7.\end{aligned}$$

If we replace each entry in the group table of $(S(\square), \circ)$ above by its image under ϕ_2, then we obtain the following table.

	3	1	5	7
3	3	1	5	7
1	1	3	7	5
5	5	7	3	1
7	7	5	1	3

This is not a group table of $(U_8, \times_8)$, because, for example, it is not true that $3 \times_8 3 = 3$. So ϕ_2 is not an isomorphism.

Exercise E99

The group tables for the groups $(S(\boxminus), \circ)$ and $(U_{12}, \times_{12})$ are given below. The elements in the borders are arranged in an order that gives the tables the same pattern, so we know that these two groups are isomorphic.

$\circ$	e	a	r	s
e	e	a	r	s
a	a	e	s	r
r	r	s	e	a
s	s	r	a	e

$(S(\boxminus), \circ)$

$\times_{12}$	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

$(U_{12}, \times_{12})$

(a) Find three different isomorphisms from $(S(\boxminus), \circ)$ to $(U_{12}, \times_{12})$.

(b) Find a one-to-one and onto mapping from $(S(\boxminus), \circ)$ to $(U_{12}, \times_{12})$ that is not an isomorphism.

Exercise E100

The group tables of the groups $(S^+(\square), \circ)$ and $(U_{10}, \times_{10})$ are given below. Again the elements in the borders are arranged in an order that gives the tables the same pattern, so we know that these two groups are isomorphic. (Recall that $(S^+(\square), \circ)$ is the group of direct symmetries of the square: see Figure 3.)

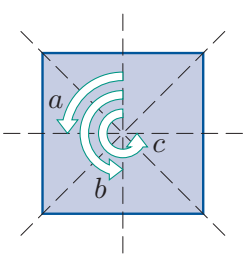

Figure 3 $S^+(\square)$

$\circ$	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

$(S^+(\square), \circ)$

$\times_{10}$	1	3	9	7
1	1	3	9	7
3	3	9	7	1
9	9	7	1	3
7	7	1	3	9

$(U_{10}, \times_{10})$

Find a one-to-one and onto mapping from $(S^+(\square), \circ)$ to $(U_{10}, \times_{10})$ that maps the identity element of $(S^+(\square), \circ)$ to the identity element of $(U_{10}, \times_{10})$ but is *not* an isomorphism.

It is permissible for the domain group and the codomain group of an isomorphism to be the same group. For example, consider the following mapping.

$$\begin{aligned} \phi : (S(\boxminus), \circ) &\longrightarrow (S(\boxminus), \circ) \\ e &\longmapsto e \\ a &\longmapsto a \\ r &\longmapsto s \\ s &\longmapsto r \end{aligned}$$

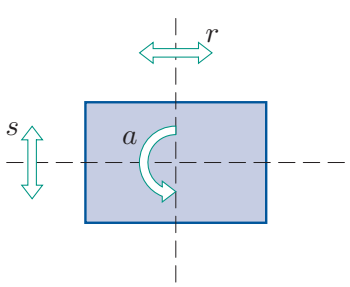

Figure 4 $S(\boxminus)$

(The non-identity symmetries of $S(\boxminus)$ are shown again in Figure 4.)

If we replace each entry in the group table of $(S(\square), \circ)$ shown on the left below with its image under ϕ, then we obtain the table on the right below.

$\circ$	e	a	r	s
e	e	a	r	s
a	a	e	s	r
r	r	s	e	a
s	s	r	a	e

$(S(\square), \circ)$

	e	a	s	r
e	e	a	s	r
a	a	e	r	s
s	s	r	e	a
r	r	s	a	e

This second table is a correct group table for $(S(\square), \circ)$, so ϕ is an isomorphism.

An isomorphism from a group to itself is called an **automorphism** of the group. Thus the mapping ϕ above is an automorphism of $(S(\square), \circ)$.

Exercise E101

Find two automorphisms of $(S(\square), \circ)$ other than the one above.

If there are no isomorphisms at all between two groups, then the groups are not isomorphic. This is always the case for two groups of different orders, because there are not even any one-to-one and onto functions between such groups. However, even if two groups have the same order, there may be no isomorphisms between them. For example, consider the groups $(S(\square), \circ)$ and $(\mathbb{Z}_4, +_4)$, whose group tables are given below.

$\circ$	e	a	r	s
e	e	a	r	s
a	a	e	s	r
r	r	s	e	a
s	s	r	a	e

$(S(\square), \circ)$

$+_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$(\mathbb{Z}_4, +_4)$

It is not possible to find a mapping from $(S(\square), \circ)$ to $(\mathbb{Z}_4, +_4)$ that transforms the group table of $(S(\square), \circ)$ into a group table for $(\mathbb{Z}_4, +_4)$. To see this, notice that in $(S(\square), \circ)$ all the elements are self-inverse, so the identity element appears in each of the four positions on the main diagonal. So every mapping from $S(\square)$ to $\mathbb{Z}_4$ will transform the group table of $(S(\square), \circ)$ into a table in which all four positions on the main diagonal contain the same element. However, in $(\mathbb{Z}_4, +_4)$ two of the elements (0 and 2) are self-inverse and the other two elements (1 and 3) are inverses of each other, so in any group table for $(\mathbb{Z}_4, +_4)$ two of the positions on the main diagonal will contain the identity element and two will not, no matter how the elements of $(\mathbb{Z}_4, +_4)$ are arranged in the table borders. Thus there is no mapping that transforms the group table of $(S(\square), \circ)$ into a group table for $(\mathbb{Z}_4, +_4)$. That is, there is no isomorphism

from $(S(\square), \circ)$ to $(\mathbb{Z}_4, +_4)$. These two groups have fundamentally different structures: they are not isomorphic.

Matching up group tables can help us investigate isomorphisms between small groups, but it is not feasible for most groups. So we need an algebraic way to express the properties that a mapping ϕ from a group $(G, \circ)$ to a group $(H, *)$ must satisfy in order to be an isomorphism. The definition that we need was given in Subsection 4.2 of Unit B2 and is restated below. It applies to both finite and infinite groups.

Definitions

Let $(G, \circ)$ and $(H, *)$ be groups. A mapping $\phi : (G, \circ) \longrightarrow (H, *)$ is an **isomorphism** if it has the following two properties:

(a) ϕ is one-to-one and onto

(b) $\phi(x \circ y) = \phi(x) * \phi(y)$ for all $x, y \in G$.

If an isomorphism $\phi : (G, \circ) \longrightarrow (H, *)$ exists, then $(G, \circ)$ and $(H, *)$ are **isomorphic**. Otherwise they are **non-isomorphic**.

We write $(G, \circ) \cong (H, *)$ (or simply $G \cong H$ when the operations $\circ$ and $*$ are clear) to assert that the groups $(G, \circ)$ and $(H, *)$ are isomorphic.

Property (a) in the definition ensures that ϕ is a one-to-one correspondence between the two groups; that is, it matches up each element of $(G, \circ)$ with exactly one element of $(H, *)$ and vice versa.

Property (b) ensures that the way that elements combine in $(G, \circ)$ matches up with the way that their corresponding elements combine in $(H, *)$. To see why it is needed, suppose that the group $(G, \circ)$ is finite, so we can construct its group table, and consider its elements x and y and their composite $x \circ y$ in the group table of $(G, \circ)$, as illustrated on the left below. In the table transformed by using a mapping $\phi : (G, \circ) \longrightarrow (H, *)$, these three elements are replaced by $\phi(x)$, $\phi(y)$ and $\phi(x \circ y)$, as illustrated on the right.

$\circ$	$\cdots$	y	$\cdots$
$\vdots$		$\vdots$	
x	$\cdots$	$x \circ y$	$\cdots$
$\vdots$		$\vdots$	

$(G, \circ)$

$\longrightarrow$

$*$	$\cdots$	$\phi(y)$	$\cdots$
$\vdots$		$\vdots$	
$\phi(x)$	$\cdots$	$\phi(x \circ y)$	$\cdots$
$\vdots$		$\vdots$	

$(H, *)$

If the table on the right is to be a correct group table for $(H, *)$, then the entry in the cell with row label $\phi(x)$ and column label $\phi(y)$ must be equal to $\phi(x) * \phi(y)$, so we must have

$$\phi(x \circ y) = \phi(x) * \phi(y).$$

This equation must hold for all elements x and y of G, which gives property (b). The property is needed for essentially the same reasons when G is infinite – the only difference is that we cannot construct a complete group table for an infinite group $(G, \circ)$.

A mapping ϕ from one group to another that satisfies property (b) is said to **preserve composites**. This property means that for any two elements from the domain group G, we can do *either* of the following and we will obtain the same answer either way.

- First compose the two elements in the domain group G using $\circ$, then map their composite using ϕ. (That is, find $\phi(x \circ y)$.)
- First map each of the two elements individually using ϕ, then compose the resulting images in the codomain group H using $*$. (That is, find $\phi(x) * \phi(y)$.)

This is illustrated in Figure 5.

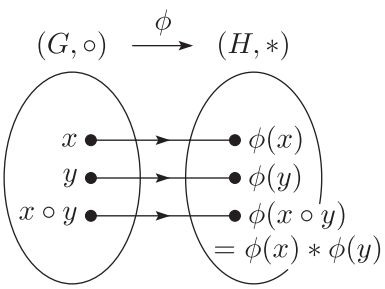

Figure 5 Preserving composites

Here is a worked exercise that demonstrates how to show that a mapping from one group to another is an isomorphism.

Worked Exercise E37

Prove that the following mapping ϕ is an isomorphism:

$$\begin{aligned} \phi : (\mathbb{Z}, +) &\longrightarrow (2\mathbb{Z}, +) \\ n &\longmapsto 2n. \end{aligned}$$

(Recall that $2\mathbb{Z} = \{2k : k \in \mathbb{Z}\}$. We know that $(2\mathbb{Z}, +)$ is a group because it is the cyclic subgroup of the group $(\mathbb{Z}, +)$ generated by the element 2.)

Solution

First we show that ϕ is one-to-one and onto.

To show that ϕ is one-to-one, suppose that m and n are elements of $\mathbb{Z}$ such that

$$\phi(m) = \phi(n).$$

Then

$$2m = 2n,$$

which gives

$$m = n.$$

Thus ϕ is one-to-one.

Also, ϕ is onto, because any element of $2\mathbb{Z}$ is of the form $2n$ where $n \in \mathbb{Z}$, and this element is the image under ϕ of the element n of $\mathbb{Z}$.

Now we show that ϕ preserves composites. It is helpful to start by taking two general elements of the domain group and writing down the equation that we have to prove in terms of these elements. This is obtained from the equation

$$\phi(x \circ y) = \phi(x) * \phi(y)$$

in the definition of an isomorphism by replacing:

x and y by general elements of the domain group,

$\circ$ by the binary operation of the domain group,

$*$ by the binary operation of the codomain group.

To check that ϕ preserves composites, let m and n be elements of $\mathbb{Z}$. We have to show that

$$\phi(m+n) = \phi(m) + \phi(n).$$

Now

$$\begin{aligned}\phi(m+n) &= 2(m+n)\\ &= 2m + 2n\\ &= \phi(m) + \phi(n).\end{aligned}$$

Thus ϕ preserves composites.

Hence ϕ is an isomorphism.

The next worked exercise provides another example of how to show that a mapping from one group to another is an isomorphism. It involves an interesting mapping: the natural logarithm function, log. The properties of this function used in the worked exercise were given in Subsection 4.2 of Unit D4 *Continuity*.

Worked Exercise E38

Show that the following mapping is an isomorphism:

$$\begin{aligned}\phi : (\mathbb{R}^+, \times) &\longrightarrow (\mathbb{R}, +)\\ x &\longmapsto \log x.\end{aligned}$$

Solution

We check that ϕ is one-to-one and onto.

The mapping ϕ (the natural logarithm function) is one-to-one.

It is also onto, because its image set is $\mathbb{R}$, which is its codomain.

We now check that ϕ preserves composites. As in Worked Exercise E37, we start by taking two general elements of the domain group, and write down the equation that has to be proved. Here the binary operations of the domain group and codomain group are $\times$ and $+$, respectively.

To check that ϕ preserves composites, let $x, y \in \mathbb{R}^+$. We have to show that

$$\phi(x \times y) = \phi(x) + \phi(y),$$

that is,

$$\log(x \times y) = \log x + \log y.$$

This is true by the properties of the function log, so ϕ preserves composites.

Hence ϕ is an isomorphism.

Worked Exercise E38 shows that the two groups $(\mathbb{R}^+, \times)$ and $(\mathbb{R}, +)$ are isomorphic.

The isomorphism in Worked Exercise E38 was widely used when doing complicated arithmetic before the days of calculators. It was easier to multiply long numbers by adding logarithms than by performing long multiplication. This was called 'using logs'.

Exercise E102

Show that the mapping

$$\begin{aligned} \phi : (\mathbb{R}, +) &\longrightarrow (\mathbb{R}^+, \times) \\ x &\longmapsto e^x \end{aligned}$$

is an isomorphism. You can use any of the properties of the exponential function given in Subsections 4.2 and 4.3 of Unit D4.

The isomorphism in Exercise E102 is the inverse function of the isomorphism in Worked Exercise E38. The inverse function of an isomorphism is always an isomorphism, as discussed later in this subsection.

In the next exercise you are asked to show that a particular mapping from a group to itself is an isomorphism. In other words, you are asked to show that this mapping is an automorphism of the group.

Exercise E103

Show that the following mapping is an isomorphism:

$$\begin{aligned}\phi : (\mathbb{Z}, +) &\longrightarrow (\mathbb{Z}, +)\\ n &\longmapsto -n.\end{aligned}$$

The next worked exercise demonstrates how to show that a mapping from a group to a group is *not* an isomorphism.

Worked Exercise E39

Explain why each of the following mappings is not an isomorphism.

(a) $\begin{aligned}\phi : (\mathbb{Z}, +) &\longrightarrow (\mathbb{R}, +)\\ n &\longmapsto 2n\end{aligned}$

(b) $\begin{aligned}\phi : (\mathbb{R}^*, \times) &\longrightarrow (\mathbb{R}^+, \times)\\ x &\longmapsto |x|\end{aligned}$

(c) $\begin{aligned}\phi : (\mathbb{Z}_4, +_4) &\longrightarrow (\mathbb{Z}_5^*, \times_5)\\ 0 &\longmapsto 1\\ 1 &\longmapsto 4\\ 2 &\longmapsto 3\\ 3 &\longmapsto 2\end{aligned}$

Solution

(a) This mapping ϕ is not onto: for example, the element π of the codomain $\mathbb{R}$ is not the image of any element in the domain $\mathbb{Z}$.

(b) This mapping ϕ is not one-to-one: for example, $\phi(2) = \phi(-2) = 2$.

(c) This mapping ϕ does not preserve composites. To preserve composites it must have the property that for all $m, n \in \mathbb{Z}_4$,

$$\phi(m +_4 n) = \phi(m) \times_5 \phi(n).$$

However, $1, 3 \in \mathbb{Z}_4$ and

$$\phi(1 +_4 3) = \phi(0) = 1,$$

whereas

$$\phi(1) \times_5 \phi(3) = 4 \times_5 2 = 3,$$

so

$$\phi(1 +_4 3) \neq \phi(1) \times_5 \phi(3).$$

Exercise E104

The following mappings are not isomorphisms. In each case, show that one of the conditions in the definition of an isomorphism fails to hold.

(a) $\phi : (\mathbb{C}^*, \times) \longrightarrow (\mathbb{R}^+, \times)$
$z \longmapsto |z|$

(b) $\phi : (\mathbb{Z}, +) \longrightarrow (\mathbb{Z}, +)$
$n \longmapsto 5n$

(c) $\phi : (\mathbb{R}^*, \times) \longrightarrow (\mathbb{R}^*, \times)$
$x \longmapsto 2^x$

In Worked Exercise E38 and Exercise E102 earlier in this subsection you saw that the mapping

$$\phi : (\mathbb{R}^+, \times) \longrightarrow (\mathbb{R}, +)$$
$$x \longmapsto \log x$$

and its inverse

$$\phi^{-1} : (\mathbb{R}, +) \longrightarrow (\mathbb{R}^+, \times)$$
$$x \longmapsto e^x$$

are both isomorphisms. In general, if ϕ is an isomorphism from a group $(G, \circ)$ to a group $(H, *)$, then ϕ^{-1} is an isomorphism from $(H, *)$ to $(G, \circ)$. This makes sense, because if the mapping ϕ 'renames' $(G, \circ)$ to $(H, *)$, then its inverse ϕ^{-1} must rename $(H, *)$ to $(G, \circ)$. This fact is stated as a proposition below, with a formal proof using the definition of an isomorphism given earlier in this subsection.

Proposition E36

Let $(G, \circ)$ and $(H, *)$ be groups. If ϕ is an isomorphism from $(G, \circ)$ to $(H, *)$, then ϕ^{-1} is an isomorphism from $(H, *)$ to $(G, \circ)$.

Proof Let $\phi : (G, \circ) \longrightarrow (H, *)$ be an isomorphism. Since ϕ is one-to-one and onto, its inverse mapping $\phi^{-1} : (H, *) \longrightarrow (G, \circ)$ exists and is also one-to-one and onto. Let h_1 and h_2 be any elements of H. Then $h_1 = \phi(g_1)$ and $h_2 = \phi(g_2)$ for some $g_1, g_2 \in G$. So

$$\begin{aligned}
\phi^{-1}(h_1 * h_2) &= \phi^{-1}(\phi(g_1) * \phi(g_2)) \\
&= \phi^{-1}(\phi(g_1 \circ g_2)) \quad \text{(since } \phi \text{ preserves composites)} \\
&= g_1 \circ g_2 \\
&= \phi^{-1}(h_1) \circ \phi^{-1}(h_2).
\end{aligned}$$

Hence ϕ^{-1} is an isomorphism, as claimed. ■

Isomorphisms of cyclic groups

You studied isomorphisms of *cyclic* groups in Subsection 4.4 of Unit B2. You met the following theorems.

Theorems B49 and B50

Let $(G, \circ)$ and $(H, *)$ be cyclic groups, generated by a and b, respectively.

- If $(G, \circ)$ and $(H, *)$ have the same finite order n, then they are isomorphic and an isomorphism is given by

$$\begin{aligned} \phi : G &\longrightarrow H \\ a^k &\longmapsto b^k \quad (k = 0, 1, \ldots, n-1). \end{aligned}$$

- If $(G, \circ)$ and $(H, *)$ both have infinite order, then they are isomorphic and an isomorphism is given by

$$\begin{aligned} \phi : G &\longrightarrow H \\ a^k &\longmapsto b^k \quad (k \in \mathbb{Z}). \end{aligned}$$

The next worked exercise illustrates how to use the first of these results to find isomorphisms between two cyclic groups of the same finite order.

Worked Exercise E40

Find two isomorphisms from $(\mathbb{Z}_4, +_4)$ to $(\mathbb{Z}_5^*, \times_5)$.

Solution

Both of these groups are cyclic groups of order 4.

To find an isomorphism between them, we first find a generator of each group.

The group $(\mathbb{Z}_4, +_4)$ is generated by 1.

To find a generator of $(\mathbb{Z}_5^*, \times_5)$, we try finding consecutive powers of 2, say, to see whether it generates the whole of $\mathbb{Z}_5^*$.

The consecutive powers of 2 in $(\mathbb{Z}_5^*, \times_5)$ starting from 2^0 are:

$$1, 2, 4, 3, \ldots.$$

All the elements of $\mathbb{Z}_5^*$ appear in this list, so 2 is a generator of $(\mathbb{Z}_5^*, \times_5)$.

To write down an isomorphism, we match up corresponding multiples/powers of the generators (depending on whether the groups are additive or multiplicative), starting by matching the zeroth

multiples/powers (the identities). This gives:

$$\begin{aligned}(\mathbb{Z}_4,+_4) &\longrightarrow (\mathbb{Z}_5^*,\times_5)\\ 0 &\longmapsto 1\\ 1 &\longmapsto 2\\ 1+_4 1 &\longmapsto 2\times_5 2\\ 1+_4 1+_4 1 &\longmapsto 2\times_5 2\times_5 2,\end{aligned}$$

that is,

$$\begin{aligned}(\mathbb{Z}_4,+_4) &\longrightarrow (\mathbb{Z}_5^*,\times_5)\\ 0 &\longmapsto 1\\ 1 &\longmapsto 2\\ 2 &\longmapsto 4\\ 3 &\longmapsto 3.\end{aligned}$$

For example, here we have matched the second *multiple* of the generator 1 in $(\mathbb{Z}_4,+_4)$, that is, $1+_4 1$, with the second *power* of the generator 2 in $(\mathbb{Z}_5^*,\times_5)$, that is, $2\times_5 2$.

Hence an isomorphism is given by

$$\begin{aligned}\phi_1 : (\mathbb{Z}_4,+_4) &\longrightarrow (\mathbb{Z}_5^*,\times_5)\\ 0 &\longmapsto 1\\ 1 &\longmapsto 2\\ 2 &\longmapsto 4\\ 3 &\longmapsto 3.\end{aligned}$$

To find a different isomorphism, we find a different generator of *one* of the groups, and match up powers/multiples of the generators in the same way as above.

The group $(\mathbb{Z}_5^*,\times_5)$ is also generated by 3 (since 3 is the inverse of 2 in $(\mathbb{Z}_5^*,\times_5)$). The consecutive powers of 3 in $(\mathbb{Z}_5^*,\times_5)$ starting from $3^0=1$ are

$$1,3,4,2,\ldots.$$

So another isomorphism is given by

$$\begin{aligned}\phi_2 : (\mathbb{Z}_4,+_4) &\longrightarrow (\mathbb{Z}_5^*,\times_5)\\ 0 &\longmapsto 1\\ 1 &\longmapsto 3\\ 2 &\longmapsto 4\\ 3 &\longmapsto 2.\end{aligned}$$

The next two exercises give you practice in finding isomorphisms between finite cyclic groups of the same order.

Exercise E105

Find an isomorphism from the group $(\mathbb{Z}_{10},+_{10})$ to the group $(\mathbb{Z}_{11}^*,\times_{11})$.

Exercise E106

Find an isomorphism from the group $(\mathbb{Z}_4,+_4)$ to the cyclic subgroup of $(\mathbb{Z}_8,+_8)$ generated by 2.

1.2 Homomorphisms

In the previous subsection you saw that an *isomorphism* is a mapping from one group to another that is one-to-one and onto and also preserves composites.

Now consider the following two mappings from groups to groups: one of them is not one-to-one and the other is not onto (as you saw in Worked Exercise E39(b) and Exercise E104(b), respectively), but they both preserve composites.

- The mapping

$$\begin{aligned} \phi : (\mathbb{R}^*, \times) &\longrightarrow (\mathbb{R}^+, \times) \\ x &\longmapsto |x| \end{aligned}$$

  is not one-to-one but is onto. It preserves composites since for all $x, y \in \mathbb{R}^*$,

$$\phi(x \times y) = |x \times y| = |x| \times |y| = \phi(x) \times \phi(y).$$

- The mapping

$$\begin{aligned} \phi : (\mathbb{Z}, +) &\longrightarrow (\mathbb{Z}, +) \\ n &\longmapsto 5n \end{aligned}$$

  is one-to-one but is not onto. It preserves composites since for all $m, n \in \mathbb{Z}$,

$$\phi(m + n) = 5(m + n) = 5m + 5n = \phi(m) + \phi(n).$$

A mapping from a group to a group that preserves composites but is not necessarily one-to-one or onto is called a *homomorphism*.

Definitions

Let $(G, \circ)$ and $(H, *)$ be groups. A mapping $\phi : (G, \circ) \longrightarrow (H, *)$ is a **homomorphism** if it has the property

$$\phi(x \circ y) = \phi(x) * \phi(y) \quad \text{for all } x, y \in G.$$

This property is called the **homomorphism property**.

Thus 'the homomorphism property' is just another name for the property of preserving composites.

A homomorphism that is both one-to-one and onto is an isomorphism.

It is important to appreciate that the homomorphism property is not likely to hold for a randomly chosen mapping between two groups. Consider any mapping ϕ from a group $(G, \circ)$ to a group $(H, *)$. In Figure 6, going from left to right *across* the diagram represents mapping from G to H using ϕ, while going *down* the diagram represents combining elements within a group, namely within $(G, \circ)$ on the left and within $(H, *)$ on the right.

Starting with two elements x and y in G, as shown in the top left-hand corner, we can combine them in $(G, \circ)$ to obtain the element $x \circ y$ of G and then map this element using ϕ to obtain the element $\phi(x \circ y)$ of H. Alternatively we can map the elements x and y individually using ϕ to obtain the elements $\phi(x)$ and $\phi(y)$ of H and then combine these elements in $(H, *)$ to obtain the element $\phi(x) * \phi(y)$ of H. In general there is no reason why there should be any connection between the elements $\phi(x \circ y)$ and $\phi(x) * \phi(y)$ of H, but if they are equal for *every* choice of x and y from G, then the mapping ϕ is a homomorphism.

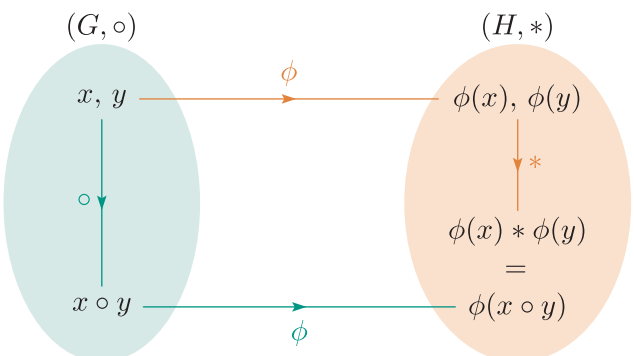

Figure 6 The homomorphism property

The worked exercise below demonstrates how to show that a mapping is a homomorphism. Doing this is just the same as checking property (b) in the definition of an isomorphism.

Worked Exercise E41

Show that the following mapping is a homomorphism:

$$\begin{aligned} \phi : (\mathbb{C}^*, \times) &\longrightarrow (\mathbb{R}^*, \times) \\ z &\longmapsto |z|. \end{aligned}$$

Solution

To show that ϕ has the homomorphism property, we start by taking two general elements of the domain group and writing down the equation that we have to prove in terms of them, being careful to use the correct binary operation on each side of the equation.

Let $z, w \in \mathbb{C}^*$. We have to show that

$$\phi(z \times w) = \phi(z) \times \phi(w).$$

Now

$$\phi(z \times w) = |z \times w| = |z| \times |w| = \phi(z) \times \phi(w),$$

by a standard property of complex numbers (given in Subsection 2.2 of Unit A2 *Number systems*). Hence ϕ is a homomorphism.

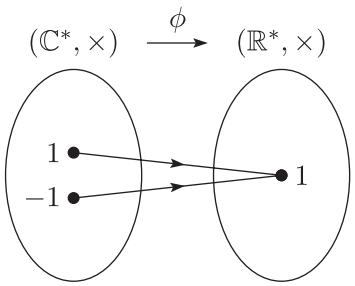

Figure 7 The homomorphism ϕ in Worked Exercise E41 is not one-to-one

Notice that the homomorphism

$$\begin{aligned}\phi : (\mathbb{C}^*, \times) &\longrightarrow (\mathbb{R}^*, \times)\\ z &\longmapsto |z|\end{aligned}$$

in Worked Exercise E41 is not an isomorphism. It is not one-to-one because, for example, the elements 1 and -1 of the domain group are both mapped by ϕ to the element 1 of the codomain group, as illustrated in Figure 7. It is not onto either, because, for example, the element -1 of the codomain group is not the image of any element of the domain group.

To show that a mapping ϕ from a group $(G, \circ)$ to a group $(H, *)$ is *not* a homomorphism, we have to find a counterexample that demonstrates that the homomorphism property does not hold for ϕ. That is, we have to find two elements $x, y \in G$ for which

$$\phi(x \circ y) \neq \phi(x) * \phi(y).$$

This is demonstrated in the next worked exercise.

Worked Exercise E42

Show that the following mapping is not a homomorphism:

$$\begin{aligned}\phi : (\mathbb{Z}, +) &\longrightarrow (\mathbb{Z}, +)\\ n &\longmapsto 2n + 3.\end{aligned}$$

Solution

The homomorphism property for ϕ is

$$\phi(m + n) = \phi(m) + \phi(n) \quad \text{for all } m, n \in \mathbb{Z}.$$

Now $1, 2 \in \mathbb{Z}$, and

$$\phi(1 + 2) = \phi(3) = 9,$$

but

$$\phi(1) + \phi(2) = 5 + 7 = 12.$$

Thus $\phi(1 + 2) \neq \phi(1) + \phi(2)$, so ϕ is not a homomorphism.

The next exercise asks you to determine whether several mappings are homomorphisms. In each part, start by writing down the homomorphism property for the mapping, try to guess whether it holds, and proceed with a proof or counterexample as appropriate. If you find it difficult to guess, then try checking the homomorphism property: if you find that you cannot complete the check, you may have gained some insight that will help you find a counterexample. When looking for a counterexample, try something simple first – remember that you need only *one* counterexample to show that a mapping is not a homomorphism.

Another useful tip is that when you are trying to check the homomorphism property equation $\phi(x \circ y) = \phi(x) * \phi(y)$, there are various ways to approach it: you can

- start with the left-hand side and show that it is equal to the right-hand side
- do the reverse
- simplify each side separately and check that you get the same answers.

The third approach is often useful in complicated cases.

Exercise E107

Determine which of the following mappings are homomorphisms.

(a) $\phi : (\mathbb{R}^*, \times) \longrightarrow (\mathbb{R}^*, \times)$
$x \longmapsto x^2$

(b) $\phi : (\mathbb{Z}, +) \longrightarrow (\mathbb{Z}, +)$
$n \longmapsto n^2$

(c) $\phi : (\mathbb{Z}_6, +_6) \longrightarrow (\mathbb{Z}_6, +_6)$
$n \longmapsto 3 \times_6 n$

(d) $\phi : (\mathbb{Z}, +) \longrightarrow (\mathbb{R}^*, \times)$
$n \longmapsto 2^n$

(e) $\phi : (\mathbb{R}, +) \longrightarrow (\mathbb{Z}_2, +_2)$

$$x \longmapsto \begin{cases} 0 & \text{if } x \text{ is rational,} \\ 1 & \text{if } x \text{ is irrational.} \end{cases}$$

(f) $\phi : (\mathbb{R}^2, +) \longrightarrow (\mathbb{R}^2, +)$
$(x, y) \longmapsto (2x - y, 6x - 3y)$

In the next worked exercise a mapping is shown to be a homomorphism by separately considering several possibilities for the natures of the elements of the domain group.

Worked Exercise E43

Let F be any figure. Show that the mapping

$$\phi : (S(F), \circ) \longrightarrow (\{1, -1\}, \times)$$

$$f \longmapsto \begin{cases} 1 & \text{if } f \text{ is a direct symmetry} \\ -1 & \text{if } f \text{ is an indirect symmetry} \end{cases}$$

is a homomorphism.

(Remember that $S(F)$ denotes the symmetry group of the figure F. You saw that $(\{1, -1\}, \times)$ is a group in Exercise B21(f) in Subsection 3.3 of Unit B1 *Symmetry and groups*.)

Solution

Let $f, g \in S(F)$. We have to show that

$$\phi(f \circ g) = \phi(f) \times \phi(g).$$

We know that a composite of two direct symmetries or two indirect symmetries is direct, and a composite of a direct symmetry and an indirect symmetry is indirect. Thus we have the following.

If f is direct and g is direct then $f \circ g$ is direct so

$$\phi(f \circ g) = 1 \quad \text{and} \quad \phi(f) \times \phi(g) = 1 \times 1 = 1.$$

If f is direct and g is indirect then $f \circ g$ is indirect so

$$\phi(f \circ g) = -1 \quad \text{and} \quad \phi(f) \times \phi(g) = 1 \times (-1) = -1.$$

If f is indirect and g is direct then $f \circ g$ is indirect so

$$\phi(f \circ g) = -1 \quad \text{and} \quad \phi(f) \times \phi(g) = (-1) \times 1 = -1.$$

If f is indirect and g is indirect then $f \circ g$ is direct so

$$\phi(f \circ g) = 1 \quad \text{and} \quad \phi(f) \times \phi(g) = (-1) \times (-1) = 1.$$

Thus in all cases $\phi(f \circ g) = \phi(f) \times \phi(g)$. Hence ϕ is a homomorphism.

Exercise E108

Let n be an integer greater than 1. Show that the mapping

$$\phi : (S_n, \circ) \longrightarrow (\mathbb{Z}_2, +_2)$$
$$f \longmapsto \begin{cases} 0 & \text{if } f \text{ is an even permutation} \\ 1 & \text{if } f \text{ is an odd permutation} \end{cases}$$

is a homomorphism.

(Remember that S_n is the symmetric group of degree n, that is, the group of all permutations of $\{1, 2, \ldots, n\}$.)

We will now look at some homomorphisms whose domain groups, and in some cases also codomain groups, are matrix groups.

Recall that the group of invertible 2×2 matrices with real entries under matrix multiplication is denoted by GL(2):

$$\mathrm{GL}(2) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in \mathbb{R},\ ad - bc \neq 0 \right\}.$$

Remember also that throughout this book we use L to denote the group of invertible 2×2 lower triangular matrices with real entries, and D to denote the group of invertible 2×2 diagonal matrices with real entries,

each under matrix multiplication:

$$L = \left\{ \begin{pmatrix} a & 0 \\ c & d \end{pmatrix} : a, c, d \in \mathbb{R},\ ad \neq 0 \right\},$$

$$D = \left\{ \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} : a, d \in \mathbb{R},\ ad \neq 0 \right\}.$$

Worked Exercise E44

Show that the following mapping is a homomorphism:

$$\phi : (L, \times) \longrightarrow (L, \times)$$
$$\begin{pmatrix} a & 0 \\ c & d \end{pmatrix} \longmapsto \begin{pmatrix} 1 & 0 \\ 0 & d^2 \end{pmatrix}.$$

Solution

Let $\mathbf{A}, \mathbf{B} \in L$. We have to show that

$$\phi(\mathbf{A} \times \mathbf{B}) = \phi(\mathbf{A}) \times \phi(\mathbf{B});$$

that is,

$$\phi(\mathbf{AB}) = \phi(\mathbf{A})\phi(\mathbf{B}).$$

Now

$$\mathbf{A} = \begin{pmatrix} r & 0 \\ t & u \end{pmatrix} \quad \text{and} \quad \mathbf{B} = \begin{pmatrix} v & 0 \\ x & y \end{pmatrix},$$

for some $r, t, u, v, x, y \in \mathbb{R}$ with $ru \neq 0$ and $vy \neq 0$.

Hence

$$\begin{aligned} \phi(\mathbf{AB}) &= \phi\left(\begin{pmatrix} r & 0 \\ t & u \end{pmatrix} \begin{pmatrix} v & 0 \\ x & y \end{pmatrix} \right) \\ &= \phi \begin{pmatrix} rv & 0 \\ tv + ux & uy \end{pmatrix} \\ &= \begin{pmatrix} 1 & 0 \\ 0 & (uy)^2 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 0 \\ 0 & u^2y^2 \end{pmatrix} \end{aligned}$$

and

$$\begin{aligned} \phi(\mathbf{A})\phi(\mathbf{B}) &= \phi \begin{pmatrix} r & 0 \\ t & u \end{pmatrix} \phi \begin{pmatrix} v & 0 \\ x & y \end{pmatrix} \\ &= \begin{pmatrix} 1 & 0 \\ 0 & u^2 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & y^2 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 0 \\ 0 & u^2y^2 \end{pmatrix}. \end{aligned}$$

Thus $\phi(\mathbf{AB}) = \phi(\mathbf{A})\phi(\mathbf{B})$. Hence ϕ is a homomorphism.

Note that for simplicity we write $\phi\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ for $\phi\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right)$.

This convention is used in the solution to Worked Exercise E44 above.

Exercise E109

Show that the following mappings are homomorphisms.

(a) $\phi : (L, \times) \longrightarrow (D, \times)$

$$\begin{pmatrix} a & 0 \\ c & d \end{pmatrix} \longmapsto \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix}$$

(b) $\phi : (L, \times) \longrightarrow (L, \times)$

$$\begin{pmatrix} a & 0 \\ c & d \end{pmatrix} \longmapsto \begin{pmatrix} a & 0 \\ a-d & d \end{pmatrix}$$

Exercise E110

Show that the following mapping is not a homomorphism:

$$\begin{aligned} \phi : (\mathrm{GL}(2), \times) &\longrightarrow (\mathrm{GL}(2), \times) \\ \mathbf{A} &\longmapsto \mathbf{A}^{-1}. \end{aligned}$$

Exercise E111

Determine whether each of the following mappings is a homomorphism, justifying your answers.

(a) $\phi : (L, \times) \longrightarrow (\mathbb{R}, +)$

$$\begin{pmatrix} a & 0 \\ c & d \end{pmatrix} \longmapsto a + d$$

(b) $\phi : (L, \times) \longrightarrow (\mathbb{R}^*, \times)$

$$\begin{pmatrix} a & 0 \\ c & d \end{pmatrix} \longmapsto a^2 d^2$$

(c) $\phi : (L, \times) \longrightarrow (\mathbb{R}^*, \times)$

$$\begin{pmatrix} a & 0 \\ c & d \end{pmatrix} \longmapsto \frac{a}{d}$$

The proposition below provides some nice examples of homomorphisms that map from an infinite group to a finite group. Here, and throughout this unit, the notation $k_{(\mathrm{mod}\ n)}$, where k is any integer and n is any integer with $n \geq 2$, is used to denote the **least residue of k modulo n**, which is the integer in $\mathbb{Z}_n$ that is congruent to k modulo n. In other words, $k_{(\mathrm{mod}\ n)}$ is the remainder of k on division by n. For example,

$$8_{(\mathrm{mod}\ 5)} = 3, \quad 5_{(\mathrm{mod}\ 5)} = 0 \quad \text{and} \quad -1_{(\mathrm{mod}\ 5)} = 4.$$

Proposition E37

For any integer $n \geq 2$, the following mapping is a homomorphism:

$$\begin{aligned} \phi : (\mathbb{Z}, +) &\longrightarrow (\mathbb{Z}_n, +_n) \\ k &\longmapsto k_{(\mathrm{mod}\ n)}. \end{aligned}$$

Proof Let n be an integer with $n \geq 2$, and let ϕ be the mapping defined above. Let $r, s \in \mathbb{Z}$. We have to show that

$$\phi(r+s) = \phi(r) +_n \phi(s),$$

that is,

$$(r+s)_{(\mathrm{mod}\ n)} = r_{(\mathrm{mod}\ n)} +_n s_{(\mathrm{mod}\ n)}.$$

Now, modulo n we have

$$\begin{aligned} r_{(\mathrm{mod}\ n)} +_n s_{(\mathrm{mod}\ n)} &\equiv r_{(\mathrm{mod}\ n)} + s_{(\mathrm{mod}\ n)} \quad \text{(by the definition of } +_n) \\ &\equiv r + s \quad \text{(since } r_{(\mathrm{mod}\ n)} \equiv r \text{ and } s_{(\mathrm{mod}\ n)} \equiv s) \\ &\equiv (r+s)_{(\mathrm{mod}\ n)} \quad \text{(by the definition of least residue).} \end{aligned}$$

But both $r_{(\mathrm{mod}\ n)} +_n s_{(\mathrm{mod}\ n)}$ and $(r+s)_{(\mathrm{mod}\ n)}$ are elements of $\mathbb{Z}_n$, so they must be equal, as required. ■

For example, the homomorphism given by Proposition E37 for $n = 3$ is as follows.

$$\begin{aligned} \phi : (\mathbb{Z}, +) &\longrightarrow (\mathbb{Z}_3, +_3) \\ &\vdots \\ -2 &\longmapsto 1 \\ -1 &\longmapsto 2 \\ 0 &\longmapsto 0 \\ 1 &\longmapsto 1 \\ 2 &\longmapsto 2 \\ 3 &\longmapsto 0 \\ 4 &\longmapsto 1 \\ &\vdots \end{aligned}$$

In the next exercise you are asked to prove a result involving homomorphisms.

Exercise E112

Prove that the mapping

$$\begin{aligned} \phi : (G, \circ) &\longrightarrow (G, \circ) \\ x &\longmapsto x \circ x \end{aligned}$$

is a homomorphism if and only if G is abelian.

The trivial homomorphism

Given any two groups $(G, \circ)$ and $(H, *)$, there is always at least one homomorphism from $(G, \circ)$ to $(H, *)$, namely the mapping that maps every element of $(G, \circ)$ to the identity element of $(H, *)$, as illustrated in Figure 8. A proof that this mapping is a homomorphism is given below. It is called the **trivial homomorphism** from $(G, \circ)$ to $(H, *)$.

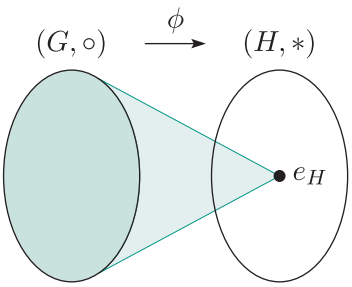

Figure 8 The trivial homomorphism from $(G, \circ)$ to $(H, *)$

Proposition E38

Let $(G, \circ)$ and $(H, *)$ be groups, and let the identity element of $(H, *)$ be e_H. Then the following mapping is a homomorphism:

$$\begin{aligned} \phi : (G, \circ) &\longrightarrow (H, *) \\ x &\longmapsto e_H. \end{aligned}$$

Proof Let $x, y \in G$. Then, since ϕ maps every element of G to e_H, we have

$$\phi(x \circ y) = e_H$$

and

$$\phi(x) * \phi(y) = e_H * e_H = e_H.$$

Thus $\phi(x \circ y) = \phi(x) * \phi(y)$. Hence ϕ is a homomorphism. ■

Linear transformations as homomorphisms

In Unit C3 you met the idea of a *linear transformation* of a vector space, as follows.

Definition

Let V and W be vector spaces. A function $t : V \longrightarrow W$ is a **linear transformation** if it satisfies the following properties.

LT1 $t(\mathbf{v}_1 + \mathbf{v}_2) = t(\mathbf{v}_1) + t(\mathbf{v}_2)$, for all $\mathbf{v}_1, \mathbf{v}_2 \in V$.

LT2 $t(\alpha \mathbf{v}) = \alpha\, t(\mathbf{v})$, for all $\mathbf{v} \in V$, $\alpha \in \mathbb{R}$.

Remember that any vector space is, in particular, a group under vector addition. So a linear transformation maps from a group to a group. It is always a homomorphism between these groups, as shown below.

Proposition E39

Let V and W be vector spaces and let $t : V \longrightarrow W$ be a linear transformation. Then t is a homomorphism from the group $(V, +)$ to the group $(W, +)$.

Proof The homomorphism property for t is

$$t(\mathbf{v}_1 + \mathbf{v}_2) = t(\mathbf{v}_1) + t(\mathbf{v}_2), \quad \text{for all } \mathbf{v}_1, \mathbf{v}_2 \in V.$$

This is the first of the two properties that t must have to be a linear transformation. Hence t is a homomorphism. ■

Thus a linear transformation is a special type of homomorphism: one whose domain group and codomain group are additive groups that are also vector spaces under some type of scalar multiplication, and that satisfies not just the homomorphism property but also a further property involving scalar multiplication (the property is that it 'preserves scalar multiples').

We can use Proposition E39 to recognise immediately that some mappings are homomorphisms. For example, consider the mapping

$$\begin{aligned} \phi : (\mathbb{R}^2, +) &\longrightarrow (\mathbb{R}^2, +) \\ (x, y) &\longmapsto (2x - y, 6x - 3y). \end{aligned}$$

You were asked to determine whether this mapping is a homomorphism in Exercise E107(f). Notice that it is a linear transformation from the vector space $\mathbb{R}^2$ to the vector space $\mathbb{R}^2$, because it is of the form

$$(x, y) \longmapsto (ax + by, cx + dy)$$

where $a, b, c, d \in \mathbb{R}$ and hence it has a matrix representation (see Theorem C41 in Unit C3). So it follows immediately from Proposition E39 that it is a homomorphism from the group $(\mathbb{R}^2, +)$ to the group $(\mathbb{R}^2, +)$. There is no need to check the homomorphism property directly, as was done in the solution to Exercise E107(f).

1.3 Properties of homomorphisms

You have seen that an isomorphism, that is, a one-to-one and onto homomorphism, preserves all the structure of its domain group. In contrast, a trivial homomorphism, which maps each element of its domain group to the identity element of its codomain group, preserves very little of the structure. These are two extremes: in general, a homomorphism preserves some, but not necessarily all, of the structure of its domain group, as you will see in this subsection.

We will start by looking at various features of a group that are preserved by homomorphisms.

Preservation of composites of two or more elements

The homomorphism property for a mapping $\phi : (G, \circ) \longrightarrow (H, *)$ is

$$\phi(x \circ y) = \phi(x) * \phi(y) \quad \text{for all } x, y \in G.$$

It is illustrated in Figure 9. This property tells us that a homomorphism preserves composites of *two* elements.

In the next exercise you are asked to prove that a homomorphism also preserves composites of *three* elements.

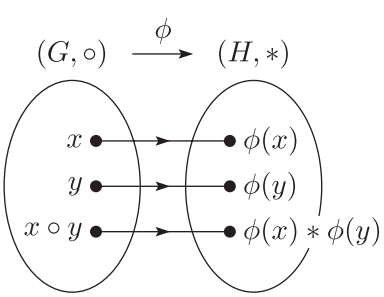

Figure 9 A homomorphism preserves composites

Exercise E113

Let $\phi : (G, \circ) \longrightarrow (H, *)$ be a homomorphism. Prove that

$$\phi(x \circ y \circ z) = \phi(x) * \phi(y) * \phi(z) \quad \text{for all } x, y, z \in G.$$

Hint: Write $x \circ y \circ z$ as $(x \circ y) \circ z$.

We can use induction to prove that a homomorphism preserves composites of any finite number of elements, as follows.

Proposition E40

Let $\phi : (G, \circ) \longrightarrow (H, *)$ be a homomorphism. If $x_1, x_2, \ldots, x_n$ are any elements of G, then

$$\phi(x_1 \circ x_2 \circ \cdots \circ x_n) = \phi(x_1) * \phi(x_2) * \cdots * \phi(x_n).$$

Proof We use induction on the number n of elements. Let $P(n)$ be the statement

$$\phi(x_1 \circ x_2 \circ \cdots \circ x_n) = \phi(x_1) * \phi(x_2) * \cdots * \phi(x_n) \quad \text{for all } x_1, x_2, \ldots, x_n \in G.$$

Then $P(1)$ is

$$\phi(x_1) = \phi(x_1) \quad \text{for all } x_1 \in G.$$

This is true.

Now suppose that $k \in \mathbb{N}$ and $P(k)$ holds; that is

$$\phi(x_1 \circ x_2 \circ \cdots \circ x_k) = \phi(x_1) * \phi(x_2) * \cdots * \phi(x_k) \quad \text{for all } x_1, x_2, \ldots, x_k \in G.$$

We prove that it follows that $P(k+1)$ holds; that is

$$\phi(x_1 \circ x_2 \circ \cdots \circ x_{k+1}) = \phi(x_1) * \phi(x_2) * \cdots * \phi(x_{k+1}) \quad \text{for all } x_1, x_2, \ldots, x_{k+1} \in G.$$

Let $x_1, x_2, \ldots, x_{k+1} \in G$. Then

$$\begin{aligned}
&\phi(x_1 \circ x_2 \circ \cdots \circ x_k \circ x_{k+1}) \\
&= \phi((x_1 \circ x_2 \circ \cdots \circ x_k) \circ x_{k+1}) \\
&= \phi(x_1 \circ x_2 \circ \cdots \circ x_k) * \phi(x_{k+1}) \\
&\qquad \text{(by the homomorphism property for } \phi) \\
&= (\phi(x_1) * \phi(x_2) * \cdots * \phi(x_k)) * \phi(x_{k+1}) \quad \text{(since } P(k) \text{ holds)} \\
&= \phi(x_1) * \phi(x_2) * \cdots * \phi(x_k) * \phi(x_{k+1}).
\end{aligned}$$

That is, $P(k+1)$ holds.

Hence, by the Principle of Mathematical Induction, the statement $P(n)$ is true for every natural number n, which proves the proposition. ■

Proposition E40 is illustrated in Figure 10.

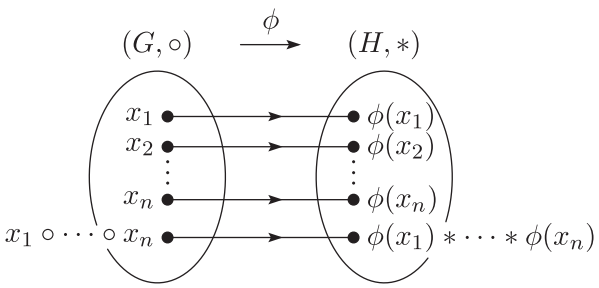

Figure 10 A homomorphism preserves composites of any finite number of elements

Preservation of the identity

You saw in Subsection 4.3 of Unit B2 that any isomorphism maps the identity element of the domain group to the identity element of the codomain group. This is true of homomorphisms in general, as illustrated in Figure 11 and proved below. We say that a homomorphism **preserves the identity**.

Throughout this unit, in discussions about an abstract homomorphism $\phi : (G, \circ) \longrightarrow (H, *)$, we will denote the identity elements of the domain group $(G, \circ)$ and codomain group $(H, *)$ by e_G and e_H, respectively, without mentioning this every time.

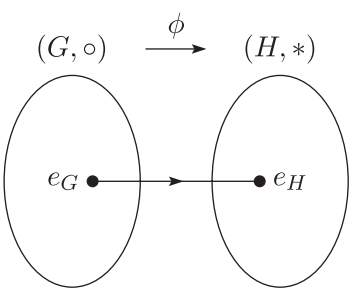

Figure 11 A homomorphism preserves the identity

Proposition E41

Let $\phi : (G, \circ) \longrightarrow (H, *)$ be a homomorphism. Then

$$\phi(e_G) = e_H.$$

Proof We have

$$e_G \circ e_G = e_G.$$

Applying the homomorphism ϕ gives

$$\phi(e_G \circ e_G) = \phi(e_G).$$

Since ϕ has the homomorphism property, this gives

$$\phi(e_G) * \phi(e_G) = \phi(e_G),$$

and hence

$$\phi(e_G) * \phi(e_G) = \phi(e_G) * e_H.$$

Applying the Left Cancellation Law now gives

$$\phi(e_G) = e_H,$$

as claimed. ■

In the next exercise you are asked to check the property in Proposition E41 for two of the homomorphisms that you met in the previous subsection.

Exercise E114

For each of the following homomorphisms ϕ, state the identity element in the domain group and the identity element in the codomain group, and check that ϕ maps one to the other.

(a) $\phi : (\mathbb{R}^*, \times) \longrightarrow (\mathbb{R}^*, \times)$, $x \longmapsto x^2$

(b) $\phi : (\mathbb{Z}_6, +_6) \longrightarrow (\mathbb{Z}_6, +_6)$, $n \longmapsto 3 \times_6 n$

(You saw that these mappings are homomorphisms in Exercise E107.)

Preservation of inverses

You saw in Subsection 4.3 of Unit B2 that an isomorphism maps elements that are inverses of each other in the domain group to elements that are inverses of each other in the codomain group. In other words, for any element x in the domain group,

the image of the inverse of x is the inverse of the image of x.

Again, this is true of homomorphisms in general, as illustrated in Figure 12 and proved below. We say that a homomorphism **preserves inverses**.

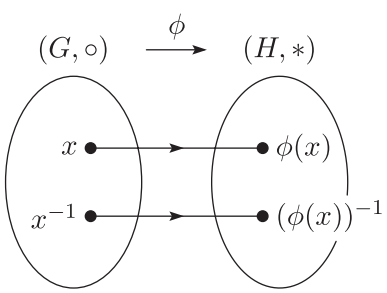

Figure 12 A homomorphism preserves inverses

Proposition E42

Let $\phi : (G, \circ) \longrightarrow (H, *)$ be a homomorphism. Then, for all $x \in G$,

$$\phi(x^{-1}) = (\phi(x))^{-1}.$$

Proof Let $x \in G$. Then

$$x \circ x^{-1} = e_G = x^{-1} \circ x.$$

Applying the homomorphism ϕ gives

$$\phi(x \circ x^{-1}) = \phi(e_G) = \phi(x^{-1} \circ x).$$

Since ϕ has the homomorphism property and since $\phi(e_G) = e_H$ by Proposition E41, this gives

$$\phi(x) * \phi(x^{-1}) = e_H = \phi(x^{-1}) * \phi(x).$$

This shows that $\phi(x^{-1})$ is the inverse of $\phi(x)$ in H; that is,

$$\phi(x^{-1}) = (\phi(x))^{-1},$$

as claimed. ■

Exercise E115

For each of the following homomorphisms ϕ and elements of their domain groups, state the inverse of the element, find the images under ϕ of the element and its inverse, and verify that these images are the inverses of each other in the codomain group.

(a) $\phi : (\mathbb{R}^*, \times) \longrightarrow (\mathbb{R}^*, \times)$
$x \longmapsto x^2$,
with the element 3 of $(\mathbb{R}^*, \times)$.

(b) $\phi : (\mathbb{Z}_6, +_6) \longrightarrow (\mathbb{Z}_6, +_6)$
$n \longmapsto 3 \times_6 n$,
with the element 4 of $(\mathbb{Z}_6, +_6)$.

(These are the same homomorphisms as in Exercise E114.)

Preservation of powers

You saw in Subsection 4.3 of Unit B2 that an isomorphism maps the powers of an element in the domain group to the corresponding powers of the image of the element in the codomain group. In other words, for any element x in the domain group and any integer n,

the image of the nth power of x is the nth power of the image of x.

Once again this is true of homomorphisms in general, as illustrated in Figure 13 and proved below. We say that a homomorphism **preserves powers**.

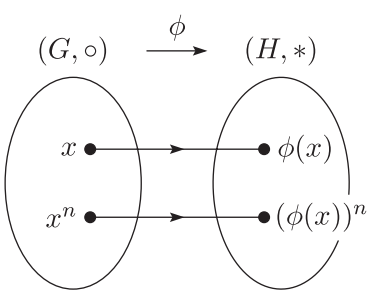

Figure 13 A homomorphism preserves powers

Proposition E43

Let $\phi : (G, \circ) \longrightarrow (H, *)$ be a homomorphism. Then, for all $x \in G$ and all $n \in \mathbb{Z}$,

$$\phi(x^n) = (\phi(x))^n.$$

Proof First we use mathematical induction to prove the result for all non-negative integers $n \geq 0$. Then we use Proposition E42 to deduce the result for negative integers.

Case 1: $n \geq 0$

Let $x \in G$ and let $P(n)$ be the statement

$$\phi(x^n) = (\phi(x))^n.$$

Then $P(0)$ is

$$\phi(x^0) = (\phi(x))^0.$$

The zeroth power of any group element is equal to the identity element of the group, so $P(0)$ is just

$$\phi(e_G) = e_H,$$

which is true, by Proposition E41.

Now let $k \geq 0$ and assume that $P(k)$ is true; that is

$$\phi(x^k) = (\phi(x))^k.$$

We have to deduce that $P(k+1)$ is true; that is,

$$\phi(x^{k+1}) = (\phi(x))^{k+1}.$$

Now

$$\begin{aligned}\phi(x^{k+1}) &= \phi(x^k \circ x)\\ &= \phi(x^k) * \phi(x) \quad \text{(since } \phi \text{ is a homomorphism)}\\ &= (\phi(x))^k * \phi(x) \quad \text{(by } P(k)\text{)}\\ &= (\phi(x))^{k+1}.\end{aligned}$$

Thus

$$P(k) \implies P(k+1), \quad \text{for } k = 0, 1, \ldots.$$

Hence, by mathematical induction, $P(n)$ is true for all $n \geq 0$. This proves the result for $n \geq 0$.

Case 2: $n < 0$

Let $x \in G$ and let $n = -m$, where $m > 0$. Then

$$\begin{aligned}\phi(x^n) &= \phi(x^{-m})\\ &= \phi((x^{-1})^m) \quad \text{(by the definition of a negative power)}\\ &= (\phi(x^{-1}))^m \quad \text{(by case 1 above, since } m > 0\text{)}\\ &= ((\phi(x))^{-1})^m \quad \text{(by Proposition E42)}\\ &= (\phi(x))^{-m} \quad \text{(by the definition of a negative power)}\\ &= (\phi(x))^n,\end{aligned}$$

as required. From cases 1 and 2 it follows that

$$\phi(x^n) = (\phi(x))^n \quad \text{for all } n \in \mathbb{Z}.$$ ■

Notice that Propositions E41 and E42 are special cases of Proposition E43, corresponding to $n = 0$ and $n = -1$, respectively.

Exercise E116

For each of the following homomorphisms ϕ and elements in their domain groups, find $\phi(g^2)$ and $(\phi(g))^2$, where g is the given element, and check that these are equal.

(a) $\phi : (\mathbb{R}^*, \times) \longrightarrow (\mathbb{R}^*, \times)$
$x \longmapsto x^2$,
with the element 3 of $(\mathbb{R}^*, \times)$.

(b) $\phi : (\mathbb{Z}_6, +_6) \longrightarrow (\mathbb{Z}_6, +_6)$
$n \longmapsto 3 \times_6 n$,
with the element 4 of $(\mathbb{Z}_6, +_6)$.

(These are the same homomorphisms as in Exercises E114 and E115.)

Homomorphisms do *not* in general preserve the *orders* of elements. This is apparent from Proposition E38, which states that if $(G, \circ)$ and $(H, *)$ are any groups, then the mapping

$$\begin{aligned} \phi : (G, \circ) &\longrightarrow (H, *) \\ x &\longmapsto e_H \end{aligned}$$

is a homomorphism (the trivial homomorphism).

However, the following theorem holds.

Theorem E44

Let $\phi : (G, \circ) \longrightarrow (H, *)$ be a homomorphism and let x be an element of finite order in G. Then the order of $\phi(x)$ is finite and divides the order of x.

This theorem can be deduced from Proposition E43: a proof is given below. First, here is a lemma that is useful in the proof.

Lemma E45

Let x be an element of a group $(G, \circ)$. If r is a positive integer such that $x^r = e$, then the order of x divides r.

Proof Suppose that $x^r = e$. Then the order of x is finite; let it be s. By the Division Theorem (Theorem A9 in Unit A2), it follows that there are integers a and b such that $r = as + b$, with $0 \leq b < s$. Now

$$\begin{aligned} e &= x^r \\ &= x^{as+b} \\ &= (x^s)^a \circ x^b \\ &= e^a \circ x^b \qquad \text{(since } x \text{ has order } s\text{)} \\ &= x^b. \end{aligned}$$

Since s is the *smallest* positive integer such that $x^s = e$, and $0 \leq b < s$, it follows that $b = 0$. Thus $r = as$ and so s divides r. ■

Now here is the proof of Theorem E44.

Proof of Theorem E44 Let the order of x be r. Then

$$\begin{aligned} (\phi(x))^r &= \phi(x^r) \quad \text{(by Proposition E43)} \\ &= \phi(e_G) \quad \text{(since } x \text{ has order } r\text{)} \\ &= e_H \quad \text{(by Proposition E41).} \end{aligned}$$

Hence the order of $\phi(x)$ is finite and by Lemma E45 it divides r. ■

Preservation of conjugates

The final result in this subsection concerns the effect of homomorphisms on conjugate elements. We describe this result by saying that homomorphisms **preserve conjugates**.

Proposition E46

Let $\phi : (G, \circ) \longrightarrow (H, *)$ be a homomorphism and let $x, y \in G$.

If x and y are conjugate in $(G, \circ)$, then $\phi(x)$ and $\phi(y)$ are conjugate in $(H, *)$.

Proof Let x and y be conjugate in $(G, \circ)$. Then

$$y = g \circ x \circ g^{-1}$$

for some $g \in G$. Hence

$$\begin{aligned}\phi(y) &= \phi(g \circ x \circ g^{-1}) \\ &= \phi(g) * \phi(x) * \phi(g^{-1}) \quad \text{(by Proposition E40)} \\ &= \phi(g) * \phi(x) * (\phi(g))^{-1} \quad \text{(by Proposition E42).}\end{aligned}$$

Since $\phi(g) \in H$, this shows that $\phi(x)$ and $\phi(y)$ are conjugate in $(H, *)$. ■

You have now seen that homomorphisms preserve all of the following:

- composites of any finite number of elements
- the identity
- inverses
- powers
- conjugates.

These properties of homomorphisms will be used to prove some important results later in this unit. They can also help you to recognise whether a mapping is a homomorphism. For example, if a mapping from one group to another does not map the identity of the first group to the identity of the second group, then you know immediately that it is not a homomorphism.

2 Images and kernels

In this section you will learn about two sets associated with a homomorphism: its *image* and its *kernel*. These are essentially the same concepts as the *image set* and *kernel* of a linear transformation, which you met in Section 4 of Unit C3. The *image set* of a function and the *image* of a function are alternative terms for the same concept.

2.1 Image of a homomorphism

You saw in Subsection 3.2 of Unit A1 *Sets, functions and vectors* what is meant by the *image set* of a function: it is the set of all elements in the codomain that are images under the function of elements in the domain. A homomorphism is just a special type of function, so it has an image set, which in group theory we call its *image*. It is defined below and illustrated in Figure 14.

Definition

Let $\phi : (G, \circ) \longrightarrow (H, *)$ be a homomorphism. The **image** (or **image set**) of ϕ is

$$\operatorname{Im}\phi = \{\phi(g) : g \in G\}.$$

It is the set of elements of the codomain group H that are images of elements in the domain group G.

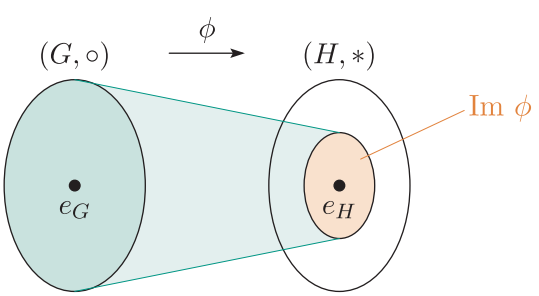

Figure 14 The image of a homomorphism

Remember that in set notation a colon (the symbol ':') means 'such that'. So the notation $\{\phi(g) : g \in G\}$ in the definition above means the set of all $\phi(g)$ such that $g \in G$.

The image of a homomorphism $\phi : (G, \circ) \longrightarrow (H, *)$ certainly contains e_H, as shown in Figure 14, because $\phi(e_G) = e_H$, by Proposition E41.

The word 'image' has other uses related to functions, of course. In particular, if ϕ is a function (such as a homomorphism) and x is an element of its domain, then $\phi(x)$ is the *image* of x under ϕ. The meaning of any particular instance of the word 'image' should be clear from the context.

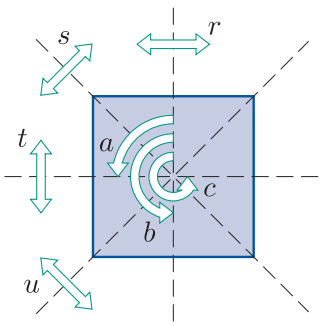

Figure 15 $S(\square)$

Worked Exercise E45

Write down the image of each of the following homomorphisms.

(a) $\phi_1 : (\mathbb{Z}_4, +_4) \longrightarrow (\mathbb{Z}_8, +_8)$

$$\begin{aligned} 0 &\longmapsto 0 \\ 1 &\longmapsto 2 \\ 2 &\longmapsto 4 \\ 3 &\longmapsto 6 \end{aligned}$$

(b) $\phi_2 : (S(\square), \circ) \longrightarrow (\mathbb{R}^*, \times)$

$$\begin{aligned} e, a, b, c &\longmapsto 1 \\ r, s, t, u &\longmapsto -1 \end{aligned}$$

(The facts that these mappings are homomorphisms follow from Exercise E106 in Subsection 1.1 and Worked Exercise E43 in Subsection 1.2, respectively. The non-identity elements of $S(\square)$ are shown in Figure 15.)

Solution

(a) The elements of the codomain group $\mathbb{Z}_8$ that are images under ϕ_1 are 0, 2, 4 and 6.

The image of ϕ_1 is

$$\operatorname{Im}\phi_1 = \{0, 2, 4, 6\}.$$

(b) The elements of the codomain group $\mathbb{R}^*$ that are images under ϕ_2 are -1 and 1.

The image of ϕ_2 is

$$\operatorname{Im}\phi_2 = \{1, -1\}.$$

The images of the homomorphisms in Worked Exercise E45 are illustrated in Figure 16.

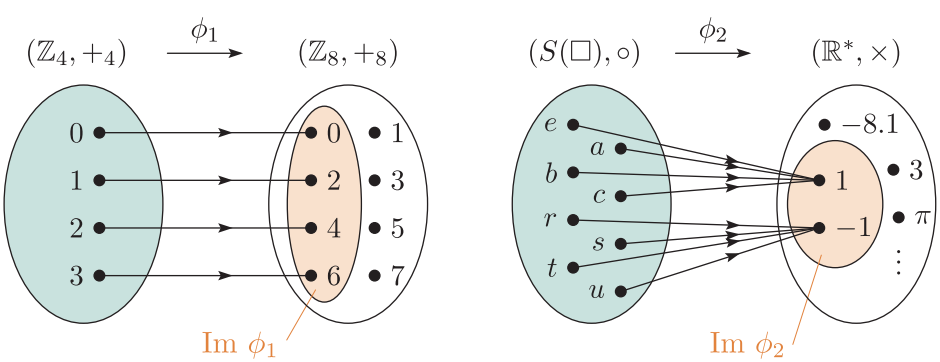

Figure 16 The images of the homomorphisms ϕ_1 and ϕ_2 in Worked Exercise E45

Exercise E117

Write down the image of each of the following homomorphisms.

(a) $\phi_3 : (S(\square), \circ) \longrightarrow (U_8, \times_8)$
$e \longmapsto 1$
$a \longmapsto 3$
$r \longmapsto 5$
$s \longmapsto 7$

(b) $\phi_4 : (\mathbb{R}^*, \times) \longrightarrow (\mathbb{R}^+, \times)$
$x \longmapsto |x|$

(The facts that these mappings are homomorphisms follow from the discussions near the starts of Subsection 1.1 and Subsection 1.2, respectively.)

The mapping ϕ_2 in Figure 16 above illustrates the fact that if $\phi : (G, \circ) \longrightarrow (H, *)$ is a homomorphism, then for each $h \in \operatorname{Im}\phi$ there may be more than one $g \in G$ such that $\phi(g) = h$. In other words, ϕ may not be one-to-one.

As with functions in general, a homomorphism $\phi : (G, \circ) \longrightarrow (H, *)$ is onto if and only if $\operatorname{Im}\phi = H$. Thus neither of the homomorphisms in Figure 16 is onto. However, both of the homomorphisms in Exercise E117 are onto.

Exercise E118

For each of the following homomorphisms, state whether it is one-to-one and whether it is onto, justifying your answers.

(a) $\phi : (\mathbb{Z}, +) \longrightarrow (\mathbb{Z}_{12}, +_{12})$
$k \longmapsto k \pmod{12}$

(b) $\phi : (\mathbb{Z}, +) \longrightarrow (\mathbb{R}^*, \times)$
$n \longmapsto 2^n$

(These mappings are homomorphisms by Proposition E37 and the solution to Exercise E107(d), respectively.)

We now look at an important property of the image of a homomorphism. The image of a homomorphism is, by definition, a subset of the codomain group of the homomorphism. It turns out that it is in fact always a *subgroup* of the codomain group.

To illustrate this, consider again the homomorphisms ϕ_1, ϕ_2, ϕ_3 and ϕ_4 from Worked Exercise E45 and Exercise E117. Their codomain groups and images are listed in Table 1 below.

Table 1 Codomain groups and images of four homomorphisms

Homomorphism	Codomain group	Image
ϕ_1	$(\mathbb{Z}_8, +_8)$	$\{0, 2, 4, 6\}$
ϕ_2	$(\mathbb{R}^*, \times)$	$\{1, -1\}$
ϕ_3	$(U_8, \times_8)$	U_8
ϕ_4	$(\mathbb{R}^+, \times)$	$\mathbb{R}^+$

The image of the homomorphism ϕ_1 is the cyclic subgroup of the codomain group generated by the element 2. Similarly, the image of the homomorphism ϕ_2 is the cyclic subgroup of the codomain group generated by the element -1. The image of the homomorphism ϕ_3 is the whole codomain group, and the same is true for the homomorphism ϕ_4. So in all four cases the image is a subgroup of the codomain group.

Here is a formal statement and proof of this property.

Theorem E47

Let $\phi : (G, \circ) \longrightarrow (H, *)$ be a homomorphism. Then $\operatorname{Im}\phi$ is a subgroup of $(H, *)$.

Proof We check that the three subgroup properties hold.

SG1 Closure

Let h_1 and h_2 be any elements of $\operatorname{Im}\phi$. Then there are elements $g_1, g_2 \in G$ such that $\phi(g_1) = h_1$ and $\phi(g_2) = h_2$. We have to show that $h_1 * h_2 \in \operatorname{Im}\phi$. Now

$$\begin{aligned} h_1 * h_2 &= \phi(g_1) * \phi(g_2) \\ &= \phi(g_1 \circ g_2) \quad \text{(since } \phi \text{ is a homomorphism).} \end{aligned}$$

Thus $h_1 * h_2$ is the image of $g_1 \circ g_2$ under ϕ, so $h_1 * h_2 \in \operatorname{Im}\phi$.

SG2 Identity

By Proposition E41, we have $\phi(e_G) = e_H$, so $e_H \in \operatorname{Im}\phi$.

SG3 Inverses

Let $h \in \operatorname{Im}\phi$. Then there is an element $g \in G$ such that $\phi(g) = h$. We have to show that $h^{-1} \in \operatorname{Im}\phi$. Now

$$\begin{aligned} h^{-1} &= (\phi(g))^{-1} \\ &= \phi(g^{-1}) \quad \text{(by Proposition E42).} \end{aligned}$$

Thus h^{-1} is the image of g^{-1} under ϕ, so $h^{-1} \in \operatorname{Im}\phi$.

Since the three subgroup properties hold for $\operatorname{Im}\phi$, it is a subgroup of $(H, *)$. ■

Structure-preserving properties of homomorphisms

When we say that a homomorphism preserves at least some of the structure of the domain group, what we mean is that at least some of the structure of the domain group is present in the image of the homomorphism, which is a group, as you have just seen.

To illustrate this, let us look again at the four homomorphisms ϕ_1, ϕ_2, ϕ_3 and ϕ_4 from Worked Exercise E45 and Exercise E117.

First consider ϕ_1, illustrated in Figure 17. This homomorphism has the additional property that it is one-to-one: each element of $\operatorname{Im}\phi$ is the image of *exactly one* element of the domain group.

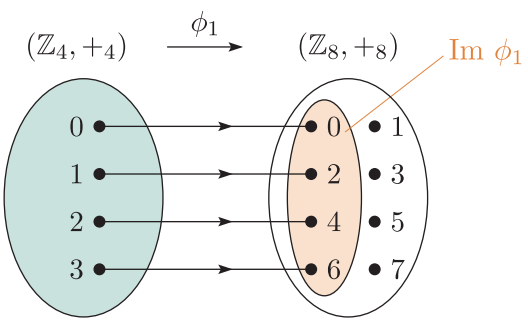

Figure 17 The homomorphism ϕ_1 and its image

It follows that if we 'shrink' the codomain of ϕ_1 from $(\mathbb{Z}_8, +_8)$ to its subgroup $\operatorname{Im}\phi = \{0, 2, 4, 6\}$, then ϕ_1 becomes an *isomorphism* from the domain group $(\mathbb{Z}_4, +_4)$ to the image $\operatorname{Im}\phi_1$. Therefore the domain group $(\mathbb{Z}_4, +_4)$ is isomorphic to $\operatorname{Im}\phi_1$. This tells us that ϕ_1 preserves *all* of the structure of the domain group.

In general, for similar reasons, any homomorphism that is one-to-one preserves all of the structure of its domain group.

Now consider the homomorphism ϕ_2, illustrated in Figure 18. It is not one-to-one: it maps the eight elements of the domain group to just two elements of the codomain group.

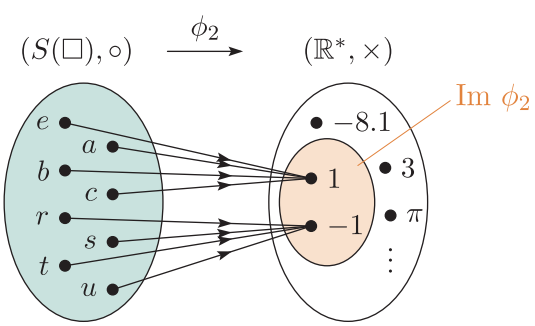

Figure 18 The homomorphism ϕ_2 and its image

It follows that this homomorphism does not preserve all of the structure of the domain group. However, it does preserve some structure, namely the structure relating to direct and indirect symmetries in the domain group, as follows.

It maps all the direct symmetries to a particular element of the codomain group, namely 1, and all the indirect symmetries to a different element of the codomain group, namely -1, and, because it preserves composites, it does this in such a way that the structure relating to composing these two types of symmetries is preserved. For example, if we compose a direct symmetry and an indirect symmetry in the domain group then we get an indirect symmetry, and correspondingly if we compose the images of these symmetries, which are 1 and -1 respectively, in the codomain group then we get -1, which corresponds to indirectness.

Next consider the homomorphism ϕ_3, illustrated in Figure 19.

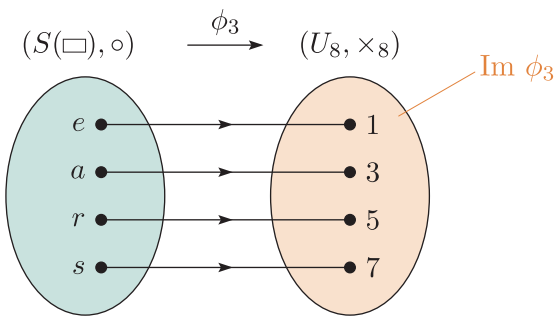

Figure 19 The homomorphism ϕ_3 and its image

This homomorphism is one-to-one, so like ϕ_1 it preserves *all* of the structure of the domain group. The domain group $S(\square)$ is isomorphic to $\operatorname{Im}\phi_3$, which in this case (since ϕ_3 is onto) is equal to the codomain group $(U_8, \times_8)$.

Finally consider the homomorphism ϕ_4, given by

$$\begin{aligned} \phi_4 : (\mathbb{R}^*, \times) &\longrightarrow (\mathbb{R}^+, \times) \\ x &\longmapsto |x|. \end{aligned}$$

It is illustrated in Figure 20, though this diagram cannot show the images of all elements in the domain group because the domain group is an infinite set.

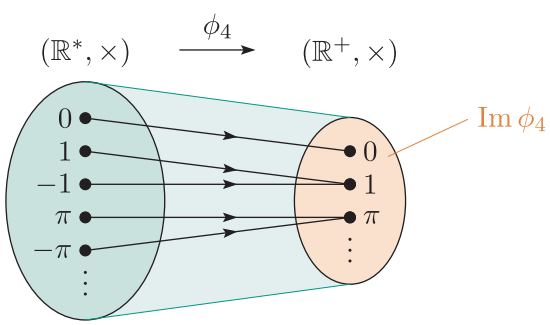

Figure 20 The homomorphism ϕ_4 and its image

Like ϕ_2, the homomorphism ϕ_4 is not one-to-one. For example, it maps both the elements 1 and -1 of the domain group to the element 1 of the image. So it does not preserve all the structure of the domain group.

However, it does preserve some of the structure, namely the structure relating to the modulus of the elements in the domain group. It maps elements of the same modulus to the same element, regardless of whether they are positive or negative and, because it preserves composites, it does this in such a way that the structure relating to composing elements of different modulus is preserved.

You saw in the discussion above that the one-to-one homomorphisms ϕ_1 and ϕ_3 preserve *all* of the structure of their domain groups. They illustrate the following general fact.

Proposition E48

Let $\phi : (G, \circ) \longrightarrow (H, *)$ be a one-to-one homomorphism, and let θ be the mapping obtained from ϕ by shrinking the codomain of ϕ to its subgroup $\operatorname{Im}\phi$. Then θ is an isomorphism, and hence $(G, \circ) \cong \operatorname{Im}\phi$.

Proof Shrinking the codomain of ϕ from $(H, *)$ to its subgroup $\operatorname{Im}\phi$ does not affect either the homomorphism property of ϕ or the fact that it is one-to-one, so θ has these properties too. However, θ is also onto, so it is an isomorphism from $(G, \circ)$ to $\operatorname{Im}\phi$, and hence $(G, \circ) \cong \operatorname{Im}\phi$. ■

Proposition E48 tells us that, as mentioned in the discussion above, every one-to-one homomorphism ϕ preserves *all* of the structure of the domain group. This structure is preserved in $\operatorname{Im}\phi$, not necessarily in the whole codomain group. (It is preserved in the whole codomain group if ϕ is also onto, that is, if ϕ is an isomorphism.)

Now let us briefly consider some particular structural features of groups that are always preserved by homomorphisms. You met several such features in Subsection 1.3, as follows:

- composites of any finite number of elements
- the identity
- inverses
- powers
- conjugates.

The next theorem states two more structural properties that are always preserved by homomorphisms.

Theorem E49

Let $\phi : (G, \circ) \longrightarrow (H, *)$ be a homomorphism.

(a) If $(G, \circ)$ is abelian, then $(\operatorname{Im}\phi, *)$ is abelian.

(b) If $(G, \circ)$ is cyclic, then $(\operatorname{Im}\phi, *)$ is cyclic.

In particular, if $(G, \circ)$ is generated by a, then $(\operatorname{Im}\phi, *)$ is generated by $\phi(a)$.

Proof

(a) Suppose that $(G, \circ)$ is abelian. We have to show that $(\operatorname{Im}\phi, *)$ is abelian. Let h_1, h_2 be any elements of $\operatorname{Im}\phi$. Then $h_1 = \phi(g_1)$ and $h_2 = \phi(g_2)$ for some $g_1, g_2 \in G$. Since $(G, \circ)$ is abelian, we have

$$g_1 \circ g_2 = g_2 \circ g_1.$$

Hence

$$\phi(g_1 \circ g_2) = \phi(g_2 \circ g_1).$$

Since ϕ is a homomorphism, this gives

$$\phi(g_1) * \phi(g_2) = \phi(g_2) * \phi(g_1);$$

that is,

$$h_1 * h_2 = h_2 * h_1.$$

This shows that $(\operatorname{Im}\phi, *)$ is abelian.

(b) Suppose that $(G, \circ)$ is cyclic, generated by a. We will show that $(\operatorname{Im}\phi, *)$ is also cyclic, generated by $\phi(a)$. Let h be any element of $\operatorname{Im}\phi$. We have to show that h can be expressed as a power of $\phi(a)$. Now $h = \phi(g)$ for some $g \in G$. Since $(G, \circ)$ is generated by a, we have

$$g = a^k$$

for some integer k. Hence

$$\phi(g) = \phi(a^k);$$

that is,

$$h = \phi(a^k).$$

By Proposition E43, this gives

$$h = (\phi(a))^k.$$

This expresses h as a power of $\phi(a)$. Thus $(\operatorname{Im}\phi, *)$ is cyclic, generated by $\phi(a)$. ■

As an illustration of Theorem E49, consider the homomorphism ϕ_1 from Worked Exercise E45, shown again in Figure 21. Its domain group is $(\mathbb{Z}_4, +_4)$, which is cyclic and hence also abelian. Hence by Theorem E49 its image $\operatorname{Im}\phi$ must also be cyclic and abelian, which indeed it is: it is the cyclic subgroup of $\mathbb{Z}_8$ generated by the element 2.

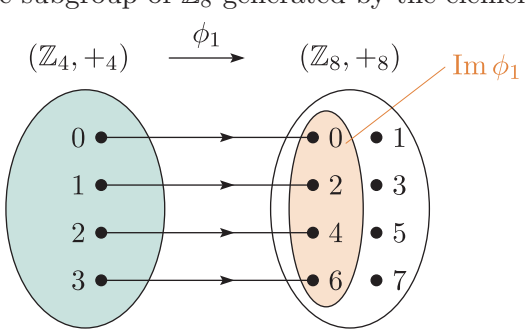

Figure 21 The homomorphism ϕ_1 and its image

Exercise E119

Explain why homomorphisms do not exist with the following properties.

(a) Domain group $(\mathbb{Z}_{12}, +_{12})$ and image $(S(\triangle), \circ)$.

(b) Domain group $(\mathbb{Z}_{12}, +_{12})$ and image $(S(\square), \circ)$.

The converses of the results in Theorem E49 do not hold. If the image of a homomorphism ϕ is abelian, then the domain group of ϕ may or may not be abelian. Similarly, if the image of a homomorphism ϕ is cyclic, then the domain group of ϕ may or may not be cyclic. For example, the image of the homomorphism ϕ_2 from Worked Exercise E45 is $(\{1, -1\}, \times)$, which is both abelian and cyclic, but the domain group of ϕ_2 is $(S(\square), \circ)$, which is neither abelian nor cyclic.

2.2 Kernel of a homomorphism

The definition of the kernel of a homomorphism is given below, and illustrated in Figure 22.

Definition

Let $\phi : (G, \circ) \longrightarrow (H, *)$ be a homomorphism. The **kernel** of ϕ is

$$\operatorname{Ker}\phi = \{g \in G : \phi(g) = e_H\}.$$

It is the set of elements of the domain group G that are mapped by ϕ to e_H.

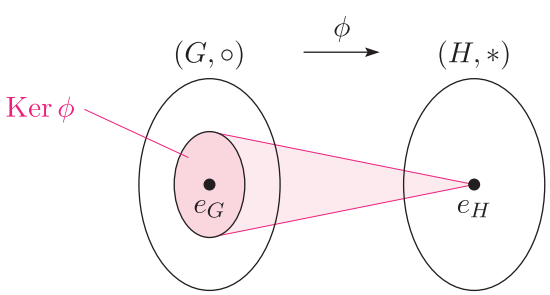

Figure 22 The kernel of a homomorphism

The kernel of a homomorphism $\phi : (G, \circ) \longrightarrow (H, *)$ certainly contains e_G, as shown in Figure 22, because $\phi(e_G) = e_H$, by Proposition E41.

The definition of the kernel of a homomorphism is essentially the same as the definition of the kernel of a linear transformation, which you met in Subsection 4.2 of Unit C3. You saw earlier that every linear transformation is also a homomorphism, so this is as you would expect.

Note that the definition of a kernel applies only to homomorphisms, not to functions in general, because the codomain of a function need not contain an identity element. This contrasts with the definition of an *image*, which does apply to all functions.

Worked Exercise E46

Write down the kernel of each of the following homomorphisms.

(a) $\phi_1 : (\mathbb{Z}_4, +_4) \longrightarrow (\mathbb{Z}_8, +_8)$

$$\begin{aligned} 0 &\longmapsto 0 \\ 1 &\longmapsto 2 \\ 2 &\longmapsto 4 \\ 3 &\longmapsto 6 \end{aligned}$$

(b) $\phi_2 : (S(\square), \circ) \longrightarrow (\mathbb{R}^*, \times)$

$$\begin{aligned} e, a, b, c &\longmapsto 1 \\ r, s, t, u &\longmapsto -1 \end{aligned}$$

(These are the same homomorphisms as in Worked Exercise E45 in the previous subsection.)

Solution

(a) The identity element of the codomain group is 0.

The only element of the domain group that is mapped to 0 by ϕ_1 is 0.

Hence

$$\operatorname{Ker}\phi = \{0\}.$$

(b) The identity element of the codomain group is 1.

The elements of the domain group that are mapped to 1 by ϕ_2 are e, a, b and c.

Hence

$$\operatorname{Ker}\phi = \{e, a, b, c\}.$$

The kernels of the homomorphisms in Worked Exercise E46 are illustrated in Figure 23. Notice that the elements of the kernel of the homomorphism ϕ_2 are the direct symmetries in $S(\square)$. That is, $\operatorname{Ker}\phi_2 = S^+(\square)$.

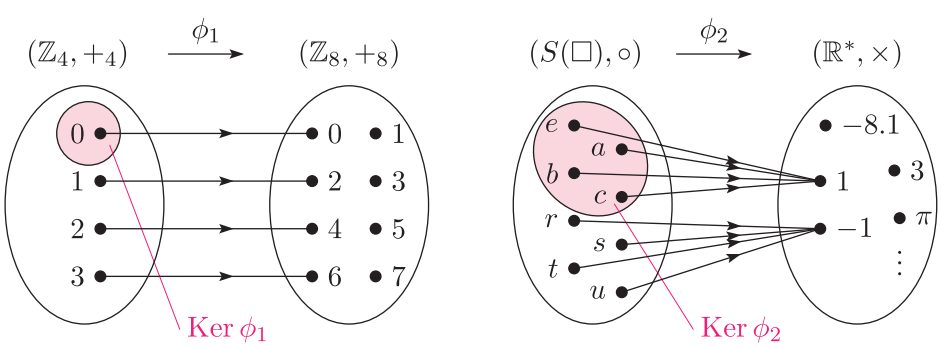

Figure 23 The kernels of the homomorphisms ϕ_1 and ϕ_2 in Worked Exercise E46

Exercise E120

For each of the following homomorphisms, write down the identity element of the codomain group, and hence write down the kernel of the homomorphism.

(a) $\phi_3 : (S(\boxminus), \circ) \longrightarrow (U_8, \times_8)$

$$\begin{aligned} e &\longmapsto 1 \\ a &\longmapsto 3 \\ r &\longmapsto 5 \\ s &\longmapsto 7 \end{aligned}$$

(b) $\phi_4 : (\mathbb{R}^*, \times) \longrightarrow (\mathbb{R}^+, \times)$

$$x \longmapsto |x|$$

(These are the same homomorphisms as in Exercise E117 in the previous subsection.)

You saw earlier that the image of a homomorphism is always a subgroup of the codomain group. The kernel has a similar property. By definition, it is a *subset* of the domain group, but in fact it is always a *subgroup* of the domain group.

To illustrate this, consider again the homomorphisms ϕ_1, ϕ_2, ϕ_3 and ϕ_4 from Worked Exercise E46 and Exercise E120. Their domain groups and kernels are summarised in Table 2.

Table 2 Domain groups and kernels of four homomorphisms

Homomorphism	Domain group	Kernel
ϕ_1	$(\mathbb{Z}_4, +)$	$\{0\}$
ϕ_2	$(S(\square), \circ)$	$S^+(\square)$
ϕ_3	$(S(\boxminus), \circ)$	$\{e\}$
ϕ_4	$(\mathbb{R}^*, \times)$	$\{1, -1\}$

For ϕ_1 and ϕ_3, the kernel contains the identity element alone, so it is the trivial subgroup of the domain group. For ϕ_2, the kernel is the subgroup $S^+(\square)$ of the domain group $S(\square)$ formed by the direct symmetries. Finally, for ϕ_4, the kernel is the cyclic subgroup of the domain group $(\mathbb{R}^*, \times)$ generated by -1. So in each case the kernel is a subgroup of the domain group.

Here is a formal statement and proof of this property.

Theorem E50

Let $\phi : (G, \circ) \longrightarrow (H, *)$ be a homomorphism. Then $\operatorname{Ker} \phi$ is a subgroup of $(G, \circ)$.

Proof We check that the three subgroup properties hold.

SG1 Closure

Let k_1 and k_2 be elements of $\operatorname{Ker}\phi$. Then $\phi(k_1) = e_H$ and $\phi(k_2) = e_H$. We have to show that $k_1 \circ k_2 \in \operatorname{Ker}\phi$.

Now

$$\begin{aligned}\phi(k_1 \circ k_2) &= \phi(k_1) * \phi(k_2) \quad \text{(since } \phi \text{ is a homomorphism)}\\ &= e_H * e_H\\ &= e_H.\end{aligned}$$

This shows that $k_1 \circ k_2 \in \operatorname{Ker}\phi$.

SG2 Identity

By Proposition E41 we have $\phi(e_G) = e_H$, so $e_G \in \operatorname{Ker}\phi$.

SG3 Inverses

Let $k \in \operatorname{Ker}\phi$. Then $\phi(k) = e_H$. We have to show that $k^{-1} \in \operatorname{Ker}\phi$.

Now

$$\begin{aligned}\phi(k^{-1}) &= (\phi(k))^{-1} \quad \text{(by Proposition E42)}\\ &= e_H^{-1}\\ &= e_H.\end{aligned}$$

Hence $k^{-1} \in \operatorname{Ker}\phi$.

This shows that $(\operatorname{Ker}\phi, \circ)$ is a subgroup of $(G, \circ)$. ■

In fact an even stronger result than Theorem E50 holds. Not only is the kernel of a homomorphism always a subgroup of the domain group, but it is always a *normal* subgroup. You can see from Table 2 that this holds for the four homomorphisms ϕ_1, ϕ_2, ϕ_3 and ϕ_4. For ϕ_1, ϕ_3 and ϕ_4, the domain group is an abelian group, so every subgroup of the domain group is normal. For ϕ_2, the domain group $S(\square)$ has order 8 and the kernel $S^+(\square)$ has order 4, so the kernel has index 2 in $S(\square)$ and is therefore normal (by Theorem E11 in Unit E1). Here is a proof of this important result.

Theorem E51

Let $\phi : (G, \circ) \longrightarrow (H, *)$ be a homomorphism. Then $\operatorname{Ker}\phi$ is a normal subgroup of $(G, \circ)$.

Proof We know from Theorem E50 that $\operatorname{Ker}\phi$ is a subgroup of $(G, \circ)$, so we have only to prove that $\operatorname{Ker}\phi$ is normal in $(G, \circ)$. To do this we use Theorem E20 (Property B) from Unit E2 *Quotient groups and conjugacy*. (This says that a subgroup H of a group G is normal in G if and only if $ghg^{-1} \in H$ for each $h \in H$ and each $g \in G$.)

Let $k \in \operatorname{Ker}\phi$ and let $g \in G$. We have to show that $g \circ k \circ g^{-1} \in \operatorname{Ker}\phi$.

Now

$$\begin{aligned}\phi(g \circ k \circ g^{-1}) &= \phi(g) * \phi(k) * \phi(g^{-1}) \quad \text{(by Proposition E40)}\\ &= \phi(g) * e_H * \phi(g^{-1}) \quad \text{(since } k \in \operatorname{Ker}\phi\text{)}\\ &= \phi(g) * \phi(g^{-1})\\ &= \phi(g) * (\phi(g))^{-1} \quad \text{(by Proposition E42)}\\ &= e_H.\end{aligned}$$

This shows that $g \circ k \circ g^{-1} \in \operatorname{Ker}\phi$. It follows that $(\operatorname{Ker}\phi, \circ)$ is normal in $(G, \circ)$, as required. ■

The next theorem gives another important property of the kernel of a homomorphism.

Theorem E52

Let $\phi : (G, \circ) \longrightarrow (H, *)$ be a homomorphism. Then ϕ is one-to-one if and only if $\operatorname{Ker}\phi = \{e_G\}$.

Proof **'Only if' part**

Suppose that ϕ is one-to-one. We know that ϕ maps e_G to e_H, by Proposition E41. Since ϕ is one-to-one, it does not map any other element of G to e_H. So $\operatorname{Ker}\phi = \{e_G\}$.

'If' part

Suppose that $\operatorname{Ker}\phi = \{e_G\}$. We have to prove that ϕ is one-to-one. To do this, suppose that $x, y \in G$ with $\phi(x) = \phi(y)$. We must show that $x = y$. Composing each side of the equation $\phi(x) = \phi(y)$ on the right with $(\phi(y))^{-1}$ (in the group $(H, *)$) gives

$$\phi(x) * (\phi(y))^{-1} = \phi(y) * (\phi(y))^{-1};$$

that is,

$$\phi(x) * (\phi(y))^{-1} = e_H.$$

Hence, by Proposition E42,

$$\phi(x) * \phi(y^{-1}) = e_H.$$

Since ϕ is a homomorphism we obtain

$$\phi(x \circ y^{-1}) = e_H.$$

Therefore $x \circ y^{-1} \in \operatorname{Ker}\phi$, and hence, since $\operatorname{Ker}\phi = \{e_G\}$, we have

$$x \circ y^{-1} = e_G.$$

Composing both sides of this equation on the right with y (in the group $(G, \circ)$) then gives

$$x \circ y^{-1} \circ y = e_G \circ y;$$

that is,

$$x = y,$$

as required. This shows that ϕ is one-to-one. ■

Theorem E52 is illustrated by the homomorphisms ϕ_1 and ϕ_2 from Worked Exercise E46, which are shown again in Figure 24. The homomorphism ϕ_1 is one-to-one and its kernel consists of the identity element alone, whereas the homomorphism ϕ_2 is not one-to-one and its kernel contains other elements as well as the identity element.

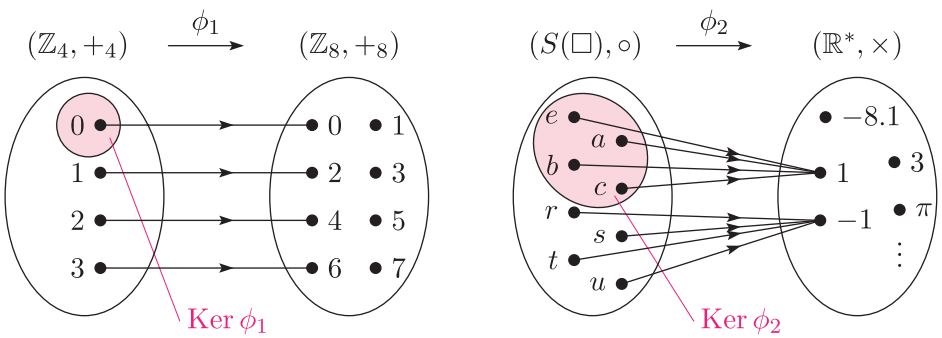

Figure 24 The kernels of the homomorphisms ϕ_1 and ϕ_2 from Worked Exercise E46

Lev Semyonovich Pontryagin

As mentioned in Unit C3, the first person to use the term *kernel* in an algebraic context was Lev Semyonovich Pontryagin (1908–1988), who used it in a paper published in 1931. Pontryagin's book *Topological Groups* (1938), translated into English in 1946, was extremely influential and is today recognised as a classic in its field. Later in his career Pontryagin turned to problems in applied mathematics.

Kernels of homomorphisms and normal subgroups

We end this subsection with an illuminating theorem that links kernels of homomorphisms and normal subgroups.

Consider any group $(G, \circ)$. By Theorem E51, the kernel of any homomorphism with domain group $(G, \circ)$ is a normal subgroup of $(G, \circ)$. In fact the converse of this statement is also true: any normal subgroup of $(G, \circ)$ is the kernel of some homomorphism with domain group $(G, \circ)$. So we have the following theorem.

Theorem E53

Let K be a subgroup of a group $(G, \circ)$. Then K is normal in G if and only if K is the kernel of a homomorphism with domain group G.

Proof

'If' part

By Theorem E51, if K is the kernel of a homomorphism with domain group G then K is normal in G.

'Only if' part

Suppose that K is normal in G. We have to show that K is the kernel of a homomorphism with domain group G.

Let ϕ be the mapping

$$\begin{aligned}\phi : (G, \circ) &\longrightarrow (G/K, \cdot) \\ x &\longmapsto xK.\end{aligned}$$

The domain of this mapping is the group G, and its codomain is the quotient group G/K, which exists because K is normal in G. So the elements of the codomain group are the cosets of K in G, and the binary operation in the codomain group is set composition, which as usual we denote by the symbol $\cdot$.

The mapping ϕ is a homomorphism, because if $x, y \in G$ then

$$\begin{aligned}\phi(x \circ y) &= (x \circ y)K \quad \text{(by the definition of } \phi) \\ &= (xK) \cdot (yK) \quad \text{(by Theorem E1 in Unit E2)} \\ &= \phi(x) \cdot \phi(y) \quad \text{(by the definition of } \phi).\end{aligned}$$

Also, the identity element of the quotient group G/K is K, so

$$\begin{aligned}\operatorname{Ker} \phi &= \{x \in G : \phi(x) = K\} \\ &= \{x \in G : xK = K\} \\ &= K.\end{aligned}$$

Hence ϕ is a homomorphism with kernel K, as required. ■

Given a group $(G, \circ)$ and one of its normal subgroups K, there are many homomorphisms with domain group $(G, \circ)$ and kernel K other than the one defined in the proof of Theorem E53.

Theorem E53 shows that kernels of homomorphisms and normal subgroups are essentially the same objects.

2.3 Finding images and kernels

You have already found the images and kernels of some homomorphisms in the previous two subsections. This subsection provides further practice in doing this, including in some more complicated cases such as when the domain group and/or codomain group are matrix groups.

Keep in mind that the image of a homomorphism is a subgroup of the *codomain group*, and the kernel is a subgroup of the *domain group*.

Remember too that usually the first step in finding the kernel of a homomorphism is to identify the identity element of the codomain group. Also, by Theorem E52, if a homomorphism $\phi : (G, \circ) \longrightarrow (H, *)$ is one-to-one, then its kernel is just $\{e_G\}$.

First try the following exercise.

Exercise E121

Find the image and kernel of each of the following homomorphisms.

(a) $\phi : (\mathbb{Z}_6, +_6) \longrightarrow (\mathbb{Z}_6, +_6)$
$n \longmapsto 3 \times_6 n$

(b) $\phi : (\mathbb{R}, +) \longrightarrow (\mathbb{R}^+, \times)$
$x \longmapsto e^x$

(c) $\phi : (\mathbb{R}^*, \times) \longrightarrow (\mathbb{R}^*, \times)$
$x \longmapsto 1$

(You saw that the mappings in parts (a) and (b) are homomorphisms in Exercise E107(c) in Subsection 1.2 and Exercise E102 in Subsection 1.1, respectively. The mapping in part (c) is a homomorphism by Proposition E38.)

If the domain group of a homomorphism is an infinite set, then we often need an algebraic argument to find its image and kernel, as demonstrated next.

Worked Exercise E47

Find the image and kernel of the homomorphism

$$\phi : (\mathbb{C}^*, \times) \longrightarrow (\mathbb{R}^*, \times)$$
$$z \longmapsto |z|.$$

(This mapping was shown to be a homomorphism in Worked Exercise E41.)

Solution

To find the image, we apply the definition, which says that for a homomorphism $\phi : (G, \circ) \longrightarrow (H, *)$,

$$\operatorname{Im}\phi = \{\phi(g) : g \in G\}.$$

For the homomorphism in the question the domain group G is $\mathbb{C}^*$. We will denote a general element of $\mathbb{C}^*$ by z, as in the question.

The image is

$$\begin{aligned}\operatorname{Im}\phi &= \{\phi(z) : z \in \mathbb{C}^*\} \\ &= \{|z| : z \in \mathbb{C}^*\}\end{aligned}$$

So $\operatorname{Im}\phi$ consists of all the values taken by $|z|$ as z takes all possible values in $\mathbb{C}^*$. That is, $\operatorname{Im}\phi$ consists of all the positive real numbers.

$$= \mathbb{R}^+.$$

To find the kernel, we first identify the identity element of the codomain group.

The identity element of the codomain group $(\mathbb{R}^*, \times)$ is 1.

Then we apply the definition of the kernel, which says that for a homomorphism $\phi : (G, \circ) \longrightarrow (H, *)$,

$$\operatorname{Ker}\phi = \{g \in G : \phi(g) = e_H\}.$$

Hence the kernel is

$$\begin{aligned}\operatorname{Ker}\phi &= \{z \in \mathbb{C}^* : \phi(z) = 1\} \\ &= \{z \in \mathbb{C}^* : |z| = 1\}\end{aligned}$$

We can simplify this specification slightly. The set of *all non-zero* complex numbers with modulus 1 is the same as the set of *all* complex numbers with modulus 1.

$$= \{z \in \mathbb{C} : |z| = 1\}.$$

This specification is acceptably simple. Since $\operatorname{Ker}\phi$ is a subset of $\mathbb{C}$, which has a geometric representation as the complex plane, we should give a geometric description of $\operatorname{Ker}\phi$ as well as the algebraic specification above.

So $\operatorname{Ker}\phi$ is the set of all complex numbers that lie on the circle with centre 0 and radius 1 in the complex plane; that is, it is the unit circle.

Exercise E122

Show that the mapping

$$\begin{aligned}\phi : (\mathbb{Z}, +) &\longrightarrow (\mathbb{Z}, +) \\ n &\longmapsto 7n\end{aligned}$$

is a homomorphism, and find its image and kernel.

The next worked exercise involves finding the image and kernel of a homomorphism whose domain group is an infinite matrix group. Remember that throughout this book we use L to denote the group of invertible 2×2 lower triangular matrices with real entries, and D to denote the group of invertible 2×2 diagonal matrices with real entries, each under matrix multiplication:

$$L = \left\{ \begin{pmatrix} a & 0 \\ c & d \end{pmatrix} : a, c, d \in \mathbb{R},\ ad \neq 0 \right\},$$

$$D = \left\{ \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} : a, d \in \mathbb{R},\ ad \neq 0 \right\}.$$

Worked Exercise E48

Find the image and kernel of the homomorphism

$$\phi : (L, \times) \longrightarrow (\mathbb{R}^*, \times)$$
$$\begin{pmatrix} a & 0 \\ c & d \end{pmatrix} \longmapsto a^2 d^2.$$

(You saw that this mapping is a homomorphism in Exercise E111(b).)

Solution

First we find the image.

Apply the definition of the image,

$$\operatorname{Im}\phi = \{\phi(g) : g \in G\},$$

to the particular homomorphism ϕ here. A general element of the domain group L is $\begin{pmatrix} a & 0 \\ c & d \end{pmatrix}$, where $a, c, d \in \mathbb{R}$ and $ad \neq 0$.

We have

$$\operatorname{Im}\phi = \left\{ \phi \begin{pmatrix} a & 0 \\ c & d \end{pmatrix} : \begin{pmatrix} a & 0 \\ c & d \end{pmatrix} \in L \right\}$$
$$= \left\{ a^2 d^2 : \begin{pmatrix} a & 0 \\ c & d \end{pmatrix} \in L \right\}.$$

Simplify the condition after the colon. (Remember that the colon means 'such that'.) What the condition tells us about the values taken by a and d is that $a, d \in \mathbb{R}$ with $ad \neq 0$.

$$= \{a^2 d^2 : a, d \in \mathbb{R},\ ad \neq 0\}.$$

As a and d run through all values in $\mathbb{R}$ such that $ad \neq 0$, the expression $a^2 d^2$ takes all possible *positive* values in $\mathbb{R}$.

$$= \mathbb{R}^+.$$

Now we find the kernel.

First identify the identity element of the codomain group. Then apply the definition of the kernel,

$$\operatorname{Ker}\phi = \{g \in G : \phi(g) = e_H\},$$

to the particular homomorphism ϕ here.

The codomain group is $(\mathbb{R}^*, \times)$, which has identity element 1, so

$$\operatorname{Ker}\phi = \left\{ \begin{pmatrix} a & 0 \\ c & d \end{pmatrix} \in L : \phi \begin{pmatrix} a & 0 \\ c & d \end{pmatrix} = 1 \right\}.$$

Simplify the condition after the colon. We can do this outside the set notation, for brevity.

Now

$$\phi\begin{pmatrix} a & 0 \\ c & d \end{pmatrix} = 1 \iff a^2d^2 = 1$$
$$\iff (ad)^2 = 1$$
$$\iff ad = \pm 1$$
$$\iff d = \pm 1/a.$$

Therefore

$$\operatorname{Ker}\phi = \left\{ \begin{pmatrix} a & 0 \\ c & d \end{pmatrix} \in L : d = \pm 1/a \right\}$$

We can simplify this expression for $\operatorname{Ker}\phi$ further by rewriting $\left\{ \begin{pmatrix} a & 0 \\ c & d \end{pmatrix} \in L : \ldots \right\}$ as $\left\{ \begin{pmatrix} a & 0 \\ c & d \end{pmatrix} : a, c, d \in \mathbb{R},\ ad \neq 0, \ldots \right\}$.

$$= \left\{ \begin{pmatrix} a & 0 \\ c & d \end{pmatrix} : a, c, d \in \mathbb{R},\ ad \neq 0,\ d = \pm 1/a \right\}$$
$$= \left\{ \begin{pmatrix} a & 0 \\ c & \pm 1/a \end{pmatrix} : a, c \in \mathbb{R},\ a \neq 0 \right\}.$$

The expression for $\operatorname{Ker}\phi$ obtained in the worked exercise above could also be written as

$$\left\{ \begin{pmatrix} a & 0 \\ c & \pm 1/a \end{pmatrix} : a \in \mathbb{R}^*,\ c \in \mathbb{R} \right\}.$$

Exercise E123

Find the image and kernel of the homomorphism

$$\phi : (L, \times) \longrightarrow (L, \times)$$
$$\begin{pmatrix} a & 0 \\ c & d \end{pmatrix} \longmapsto \begin{pmatrix} 1 & 0 \\ 0 & d^2 \end{pmatrix}.$$

(You saw that this mapping is a homomorphism in Worked Exercise E44 in Subsection 1.2.)

Exercise E124

Find the kernel of the homomorphism

$$\phi : (L, \times) \longrightarrow (D, \times)$$
$$\begin{pmatrix} a & 0 \\ c & d \end{pmatrix} \longmapsto \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix}.$$

(Its image is found in the next worked exercise. You saw that this mapping is a homomorphism in Exercise E109(a) in Subsection 1.2.)

The next worked exercise reminds you about a different type of algebraic argument that is sometimes useful when you want to find the image of a homomorphism. If you suspect that the image is the *whole codomain group* – that is, the homomorphism is *onto* – then you can verify this by using an algebraic argument to prove that every element of the codomain group is the image of some element of the domain group.

Worked Exercise E49

Find the image of the homomorphism

$$\phi : (L, \times) \longrightarrow (D, \times)$$
$$\begin{pmatrix} a & 0 \\ c & d \end{pmatrix} \longmapsto \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix}.$$

(You were asked to find the kernel of this homomorphism in Exercise E124.)

Solution

We suspect that this homomorphism is onto, so we try to use an algebraic argument to prove that it is. We have to show that every element of the codomain group is the image under ϕ of some element of the domain group.

We show that ϕ is onto. A general element of the codomain group $(D, \times)$ is

$$\begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix},$$

where $a, d \in \mathbb{R}$ and $ad \neq 0$.

Find *any* element of the domain group that is mapped by ϕ to this matrix. Remember to check that the element that you have found satisfies all the conditions to be in the domain group.

The matrix

$$\begin{pmatrix} a & 0 \\ 1 & d \end{pmatrix}$$

is an element of the domain group $(L, \times)$, because it is lower triangular and its determinant is ad which is non-zero, and

$$\phi \begin{pmatrix} a & 0 \\ 1 & d \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix}.$$

Thus ϕ is onto, and hence

$$\operatorname{Im} \phi = (D, \times).$$

Exercise E125

Show that the following homomorphism is onto and hence write down its image:

$$\phi : (L, \times) \longrightarrow (\mathbb{R}^*, \times)$$
$$\begin{pmatrix} a & 0 \\ c & d \end{pmatrix} \longmapsto \frac{a}{d}.$$

(You saw that this mapping is a homomorphism in Exercise E111(c) in Subsection 1.2.)

Finally, here is one more possible approach to keep in mind when you want to find the image or kernel of a homomorphism. You could try making an informed guess about what the image or kernel is, and then confirm your guess by applying Strategy A1 from Unit A1. This strategy says that to show that two sets are equal, show that each set is a subset of the other. Thus if you think that $\operatorname{Im}\phi$ is a particular set S, say, then you can confirm this by showing that $\operatorname{Im}\phi \subseteq S$ and $S \subseteq \operatorname{Im}\phi$. Here is an example; it involves the same homomorphism as in Worked Exercise E48, but it determines the image of the homomorphism in the way just described.

Worked Exercise E50

Find the image of the homomorphism

$$\phi : (L, \times) \longrightarrow (\mathbb{R}^*, \times)$$
$$\begin{pmatrix} a & 0 \\ c & d \end{pmatrix} \longmapsto a^2d^2.$$

Solution

Make an informed guess about what the image is, then confirm it. The specification of ϕ suggests that $\operatorname{Im}\phi = \mathbb{R}^+$.

We show that $\operatorname{Im}\phi = \mathbb{R}^+$.

First we show that $\operatorname{Im}\phi \subseteq \mathbb{R}^+$. Let $r \in \operatorname{Im}\phi$. Then

$$r = \phi \begin{pmatrix} a & 0 \\ c & d \end{pmatrix},$$

where $a, c, d \in \mathbb{R}$ and $ad \neq 0$. This gives

$$r = a^2d^2.$$

Since $a, d \in \mathbb{R}$ and $ad \neq 0$, it follows that $r > 0$ and hence $r \in \mathbb{R}^+$. Therefore $\operatorname{Im}\phi \subseteq \mathbb{R}^+$.

Now we show that $\mathbb{R}^+ \subseteq \operatorname{Im}\phi$. Let $r \in \mathbb{R}^+$. Then r is the image under ϕ of the matrix

$$\begin{pmatrix} 1 & 0 \\ 0 & \sqrt{r} \end{pmatrix},$$

since

$$\phi\begin{pmatrix} 1 & 0 \\ 0 & \sqrt{r} \end{pmatrix} = 1^2\left(\sqrt{r}\right)^2 = r.$$

Also

$$\begin{pmatrix} 1 & 0 \\ 0 & \sqrt{r} \end{pmatrix} \in L$$

because it is of the form

$$\begin{pmatrix} a & 0 \\ c & d \end{pmatrix}$$

with $a = 1$, $c = 0$, $d = \sqrt{r}$ and $ad = 1\sqrt{r} = \sqrt{r} \neq 0$. Hence $r \in \operatorname{Im}\phi$. Therefore $\mathbb{R}^+ \subseteq \operatorname{Im}\phi$.

Since $\operatorname{Im}\phi \subseteq \mathbb{R}^+$ and $\mathbb{R}^+ \subseteq \operatorname{Im}\phi$, it follows that $\operatorname{Im}\phi = \mathbb{R}^+$.

Exercise E126

Use the method of Worked Exercise E50 to show that the image of the homomorphism

$$\begin{aligned} \phi : (\mathbb{R}^*, \times) &\longrightarrow (\mathbb{R}^*, \times) \\ x &\longmapsto x^2 \end{aligned}$$

is $\mathbb{R}^+$.

(You saw that ϕ is a homomorphism in Exercise E107(a) in Subsection 1.2.)

3 The First Isomorphism Theorem

This section leads up to and covers the *First Isomorphism Theorem*, an important theorem in group theory that links the ideas of homomorphisms and quotient groups.

3.1 Cosets of the kernel of a homomorphism

You saw in the last section that the kernel of a homomorphism is a *normal* subgroup of its domain group. Thus the left cosets of the kernel in the domain group are the same as its right cosets, and we refer to them simply as cosets. In this subsection you will meet an important property of the cosets of the kernel of a homomorphism.

Here is an example that illustrates this property. Consider the mapping

$$\begin{aligned}\phi : (\mathbb{Z}_{12}, +_{12}) &\longrightarrow (\mathbb{Z}_{12}, +_{12}) \\ n &\longmapsto 3 \times_{12} n.\end{aligned}$$

This is a homomorphism because, for any $m, n \in \mathbb{Z}_{12}$,

$$\begin{aligned}\phi(m +_{12} n) &= 3 \times_{12} (m +_{12} n) \\ &= (3 \times_{12} m) +_{12} (3 \times_{12} n) \\ &= \phi(m) +_{12} \phi(n).\end{aligned}$$

Let us find its kernel. The identity element of the codomain group is 0, so

$$\begin{aligned}\operatorname{Ker}\phi &= \{n \in \mathbb{Z}_{12} : \phi(n) = 0\} \\ &= \{n \in \mathbb{Z}_{12} : 3 \times_{12} n = 0\} \\ &= \{0, 4, 8\}.\end{aligned}$$

We will now find the cosets of $\operatorname{Ker}\phi$ in the domain group $(\mathbb{Z}_{12}, +_{12})$. Using our usual method for finding cosets, we find that they are

$$\begin{aligned}\operatorname{Ker}\phi &= \{0, 4, 8\}, \\ 1 + \operatorname{Ker}\phi &= \{1, 5, 9\}, \\ 2 + \operatorname{Ker}\phi &= \{2, 6, 10\}, \\ 3 + \operatorname{Ker}\phi &= \{3, 7, 11\}.\end{aligned}$$

Let us now find the images under ϕ of the elements of the domain group $(\mathbb{Z}_{12}, +_{12})$, one coset at a time.

The image under ϕ of each element of $\operatorname{Ker}\phi$ itself is, of course, 0.

Now we find the images of the elements in the second coset above:

$$\phi(1) = 3, \quad \phi(5) = 3, \quad \phi(9) = 3.$$

Each element of this coset has the *same* image, namely 3.

A similar property is true for each of the other two cosets:

$$\begin{aligned}\phi(2) = \phi(6) = \phi(10) = 6, \\ \phi(3) = \phi(7) = \phi(11) = 9.\end{aligned}$$

Thus whenever two elements of the domain group $(\mathbb{Z}_{12}, +_{12})$ lie in the *same* coset of $\operatorname{Ker}\phi$, they have the *same* image under ϕ, whereas whenever they lie in *different* cosets, they have *different* images. This is illustrated in Figure 25.

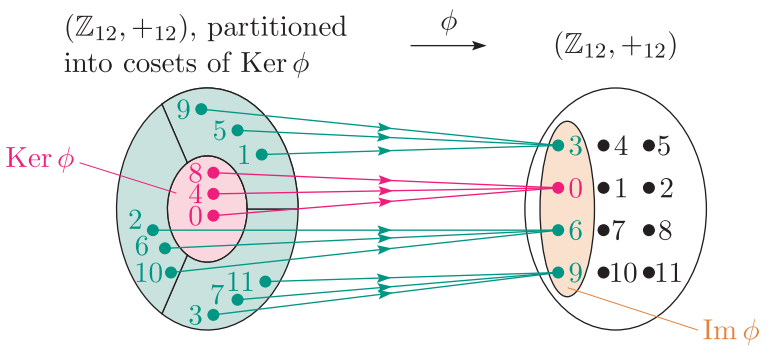

Figure 25 The homomorphism $\phi : (\mathbb{Z}_{12}, +_{12}) \longrightarrow (\mathbb{Z}_{12}, +_{12})$ with rule $n \longmapsto 3 \times_{12} n$

This finding, for this particular homomorphism ϕ, is a particular example of the following general theorem.

Theorem E54

Let $\phi : (G, \circ) \longrightarrow (H, *)$ be a homomorphism, and let x and y be any elements of G. Then

x and y have the same image under ϕ

if and only if

x and y lie in the same coset of $\operatorname{Ker}\phi$ in G.

Proof

'If' part

Suppose that x and y lie in the same coset of $\operatorname{Ker}\phi$ in G. We have to show that $\phi(x) = \phi(y)$.

Since x and y lie in the same coset of $\operatorname{Ker}\phi$ in G, we have

$$y \in x \operatorname{Ker}\phi.$$

Hence there is an element k in $\operatorname{Ker}\phi$ such that

$$y = x \circ k.$$

Therefore

$$\begin{aligned} \phi(y) &= \phi(x \circ k) \\ &= \phi(x) * \phi(k) \quad \text{(since } \phi \text{ is a homomorphism)} \\ &= \phi(x) * e_H \quad \text{(since } k \in \operatorname{Ker}\phi\text{)} \\ &= \phi(x), \end{aligned}$$

as required.

'Only if' part

Suppose that $\phi(x) = \phi(y)$. We have to show that x and y lie in the same coset of $\operatorname{Ker}\phi$ in G.

Consider the image of the element $x^{-1} \circ y$ under ϕ. We have

$$\begin{aligned}\phi(x^{-1} \circ y) &= \phi(x^{-1}) * \phi(y) \quad \text{(since } \phi \text{ is a homomorphism)}\\ &= (\phi(x))^{-1} * \phi(y) \quad \text{(by Proposition E42)}\\ &= (\phi(x))^{-1} * \phi(x) \quad \text{(since } \phi(x) = \phi(y))\\ &= e_H.\end{aligned}$$

Thus $x^{-1} \circ y$ belongs to $\operatorname{Ker}\phi$. Hence there is an element k in $\operatorname{Ker}\phi$ such that

$$x^{-1} \circ y = k.$$

Composing both sides of this equation on the left by x gives

$$y = x \circ k,$$

which shows that

$$y \in x \operatorname{Ker}\phi.$$

That is, x and y lie in the same coset of $\operatorname{Ker}\phi$, as required. ■

Theorem E54 tells us that, for any homomorphism, the sets of elements in the domain group that have the same image are precisely the cosets of the kernel. This means that

> if we collect together the domain group elements according to their images under the homomorphism, then we have the cosets of the kernel;

and that, conversely,

> if we find the cosets of the kernel, then we have the sets of domain group elements that have the same image under the homomorphism.

In the next exercise you are asked to check this for a particular homomorphism ϕ similar to the one that was used as an example at the start of this subsection.

Exercise E127

Consider the mapping

$$\begin{aligned}\phi : (\mathbb{Z}_{12}, +_{12}) &\longrightarrow (\mathbb{Z}_{12}, +_{12})\\ n &\longmapsto 2 \times_{12} n.\end{aligned}$$

(a) Show that ϕ is a homomorphism.

(b) Find $\operatorname{Ker}\phi$ and its cosets in $(\mathbb{Z}_{12}, +_{12})$.

(c) Find the partition of $\mathbb{Z}_{12}$ obtained by collecting together the elements of $\mathbb{Z}_{12}$ that have the same image under ϕ. Check that this partition is the same as that found in part (b).

Theorem E54 applies to homomorphisms with infinite domain groups and/or infinite codomain groups, as well as to those with finite domain groups and finite codomain groups, as illustrated in the next exercise.

Exercise E128

Consider the mapping

$$\phi : (\mathbb{Z}, +) \longrightarrow (\mathbb{Z}_5, +_5)$$
$$k \longmapsto k \pmod 5.$$

It is a homomorphism by Proposition E37 in Subsection 1.2. (Remember that, in this unit, the notation $k \pmod n$ denotes the integer in $\mathbb{Z}_n$ that is congruent to k modulo n.)

(a) Find $\operatorname{Ker}\phi$ and its cosets in $(\mathbb{Z}, +)$.

(b) Find the partition of $\mathbb{Z}$ obtained by collecting together elements of $\mathbb{Z}$ that have the same image under ϕ. Check that this partition is the same as that in part (a).

The following theorem from Subsection 2.2 can be viewed as a corollary of Theorem E54, as shown by its alternative proof below.

Theorem E52

Let $\phi : (G, \circ) \longrightarrow (H, *)$ be a homomorphism. Then ϕ is one-to-one if and only if $\operatorname{Ker}\phi = \{e_G\}$.

Proof (using Theorem E54)

'If' part

Suppose that $\operatorname{Ker}\phi = \{e_G\}$. Then each coset of $\operatorname{Ker}\phi$ consists of a single element (since by Proposition E3 in Unit E1 each coset contains the same number of elements as $\operatorname{Ker}\phi$). So, by Theorem E54, each element of G has a distinct image under ϕ. That is, ϕ is one-to-one.

'Only if' part

Suppose that ϕ is one-to-one. Then each element of G has a distinct image under ϕ. So, by Theorem E54, each coset of $\operatorname{Ker}\phi$, and in particular $\operatorname{Ker}\phi$ itself, contains only a single element. The single element of $\operatorname{Ker}\phi$ is e_G, since certainly $e_G \in \operatorname{Ker}\phi$. Thus $\operatorname{Ker}\phi = \{e_G\}$. ■

3.2 The First Isomorphism Theorem

In this subsection you will meet the *First Isomorphism Theorem*, an important theorem in group theory. There is also a *Second Isomorphism Theorem* and a *Third Isomorphism Theorem* in group theory, but these theorems are outside the scope of this module.

To understand what the First Isomorphism Theorem tells us, consider any homomorphism $\phi : (G, \circ) \longrightarrow (H, *)$. You have seen that $\operatorname{Ker}\phi$ is a normal subgroup of the domain group $(G, \circ)$, and that the sets of elements of $(G, \circ)$ that have the same image under ϕ are precisely the cosets of $\operatorname{Ker}\phi$ in $(G, \circ)$. It follows that we can use the homomorphism ϕ to define a new mapping, say f, whose domain is the set of cosets of $\operatorname{Ker}\phi$ in $(G, \circ)$, whose codomain is $\operatorname{Im}\phi$, and whose rule is

$$\text{coset} \longmapsto \text{element of } \operatorname{Im}\phi \text{ that is the image under } \phi \text{ of each element of the coset.}$$

This mapping f is illustrated in Figure 26. Note in particular that the elements of its domain are *whole cosets*, not individual elements of $(G, \circ)$.

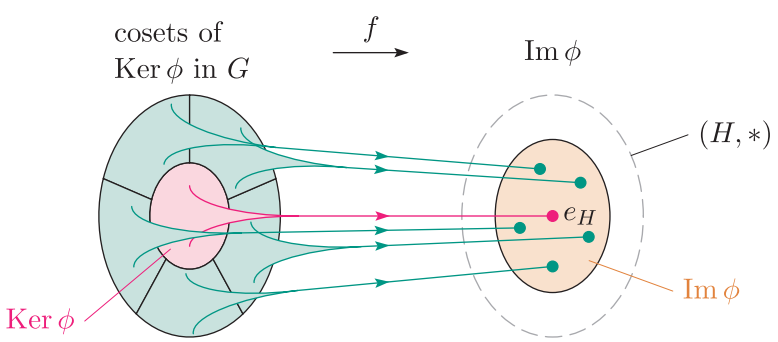

Figure 26 The mapping f obtained from the homomorphism ϕ

Since the cosets of $\operatorname{Ker}\phi$ are the elements of the quotient group $G/\operatorname{Ker}\phi$, and $\operatorname{Im}\phi$ is a group, the domain and codomain of the mapping f are both *groups*. The First Isomorphism Theorem states that this mapping f is in fact always an *isomorphism*. Thus, for any homomorphism $\phi : (G, \circ) \longrightarrow (H, *)$, the quotient group $G/\operatorname{Ker}\phi$ is isomorphic to $\operatorname{Im}\phi$.

For instance, consider the homomorphism ϕ that was used as an example at the start of the previous subsection:

$$\begin{aligned} \phi : (\mathbb{Z}_{12}, +_{12}) &\longrightarrow (\mathbb{Z}_{12}, +_{12}) \\ n &\longmapsto 3 \times_{12} n. \end{aligned}$$

You saw that for this homomorphism the cosets of $\operatorname{Ker}\phi$ are

$$\{0, 4, 8\}, \quad \{1, 5, 9\}, \quad \{2, 6, 10\}, \quad \{3, 7, 11\}.$$

You also saw that ϕ maps all the elements of the first coset (which is $\operatorname{Ker}\phi$ itself) to 0, all the elements of the second coset to 3, all the elements of the third coset to 6 and all the elements of the fourth coset to 9. The mapping f obtained from ϕ as described above is therefore

$$\begin{aligned} f : \mathbb{Z}_{12}/\operatorname{Ker}\phi &\longrightarrow \operatorname{Im}\phi \\ \{0,4,8\} &\longmapsto 0 \\ \{1,5,9\} &\longmapsto 3 \\ \{2,6,10\} &\longmapsto 6 \\ \{3,7,11\} &\longmapsto 9. \end{aligned}$$

It is illustrated in Figure 27.

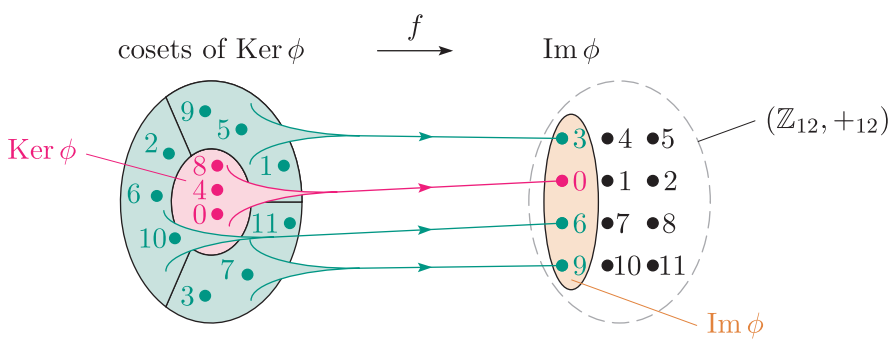

Figure 27 The mapping f obtained from the homomorphism $\phi : (\mathbb{Z}_{12}, +_{12}) \longrightarrow (\mathbb{Z}_{12}, +_{12})$ with rule $n \longmapsto 3 \times_{12} n$

The First Isomorphism Theorem tells us that this mapping f is in fact an isomorphism, and hence $\mathbb{Z}_{12}/\operatorname{Ker}\phi \cong \operatorname{Im}\phi$; that is,

$$\mathbb{Z}_{12}/\operatorname{Ker}\phi \cong (\{0,3,6,9\}, +_{12}).$$

Here is the formal statement and proof of the First Isomorphism Theorem.

Theorem E55 First Isomorphism Theorem

Let $\phi : (G, \circ) \longrightarrow (H, *)$ be a homomorphism. Then the mapping

$$\begin{aligned} f : G/\operatorname{Ker}\phi &\longrightarrow \operatorname{Im}\phi \\ x \operatorname{Ker}\phi &\longmapsto \phi(x) \end{aligned}$$

is an isomorphism, so

$$G/\operatorname{Ker}\phi \cong \operatorname{Im}\phi.$$

Proof In this proof we will denote $\operatorname{Ker}\phi$ simply by K, for brevity.

The mapping f maps each coset of K to the image under ϕ of any element x of the coset. This is a valid definition of a mapping because, by Theorem E54, all the elements of a coset of K have the *same* image under ϕ. To show that f is an isomorphism, we have to show that it is one-to-one and onto and that it has the homomorphism property.

Theorem E54 tells us that elements from *different* cosets of K have *different* images under ϕ, so f is one-to-one.

Also, f is onto, because each element $\phi(x)$ of $\operatorname{Im}\phi$ is the image under f of the coset xK.

It remains to prove that f has the homomorphism property. Let xK and yK be cosets in G/K. We have to show that

$$f(xK \cdot yK) = f(xK) * f(yK)$$

where $\cdot$ denotes set composition. Now

$$\begin{aligned} f(xK \cdot yK) &= f((x \circ y)K) \quad \text{(by Theorem E1 in Unit E2)} \\ &= \phi(x \circ y) \quad \text{(by the definition of } f\text{)} \\ &= \phi(x) * \phi(y) \quad \text{(since } \phi \text{ is a homomorphism)} \\ &= f(xK) * f(yK) \quad \text{(by the definition of } f\text{)}. \end{aligned}$$

Hence f has the homomorphism property.

Thus f is an isomorphism from the quotient group G/K to $\operatorname{Im}\phi$. Therefore $G/K \cong \operatorname{Im}\phi$. ■

The First Isomorphism Theorem is illustrated in Figure 28. This diagram shows a homomorphism ϕ and the isomorphism f obtained from ϕ as specified in the theorem. (In the diagram, as in earlier diagrams, $\operatorname{Ker}\phi$ is shown as having finitely many cosets in the domain group $(G, \circ)$, but of course there could be infinitely many.)

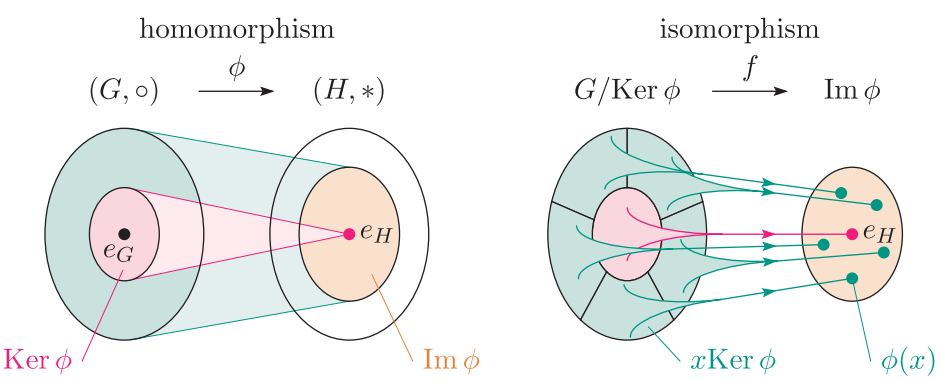

Figure 28 A homomorphism ϕ and the isomorphism f obtained from it

In the rest of this subsection we will look at one way in which we can apply the First Isomorphism Theorem, as follows.

You have seen that if N is a normal subgroup of a group G, then it can be helpful to identify a familiar, standard group that is isomorphic to the quotient group G/N. Since isomorphic groups have the same structure, this can give us useful information about the quotient group. There is a list of standard groups, both finite and infinite, in the module Handbook.

We can sometimes use the First Isomorphism Theorem to help us identify a familiar, standard group that is isomorphic to a quotient group $G/\operatorname{Ker}\phi$, where $\phi : (G, \circ) \longrightarrow (H, *)$ is a homomorphism. Here is an example.

Worked Exercise E51

Consider the mapping

$$\begin{aligned}\phi : (\mathbb{C}^*, \times) &\longrightarrow (\mathbb{R}^*, \times)\\ z &\longmapsto |z|.\end{aligned}$$

You saw that this mapping is a homomorphism in Worked Exercise E41 in Subsection 1.2. You also saw in Worked Exercise E47 in Subsection 2.3 that

$$\operatorname{Im}\phi = \mathbb{R}^+$$

and

$$\operatorname{Ker}\phi = \{z \in \mathbb{C} : |z| = 1\}.$$

State a standard group isomorphic to the quotient group $\mathbb{C}^*/\operatorname{Ker}\phi$.

Solution

Use the First Isomorphism Theorem. Remember that $\operatorname{Im}\phi$ is a subgroup of the codomain group, so it has the same binary operation as the codomain group.

By the First Isomorphism Theorem,

$$\mathbb{C}^*/\operatorname{Ker}\phi \cong \operatorname{Im}\phi,$$

so

$$\mathbb{C}^*/\operatorname{Ker}\phi \cong (\mathbb{R}^+, \times).$$

So a standard group isomorphic to $\mathbb{C}^*/\operatorname{Ker}\phi$ is $(\mathbb{R}^+, \times)$.

Exercise E129

Consider the mapping

$$\begin{aligned}\phi : (\mathbb{R}^2, +) &\longrightarrow (\mathbb{R}, +)\\ (x, y) &\longmapsto x + y.\end{aligned}$$

(a) Show that ϕ is a homomorphism.

(b) Find $\operatorname{Im}\phi$ and $\operatorname{Ker}\phi$.

(c) State a standard group isomorphic to the quotient group $\mathbb{R}^2/\operatorname{Ker}\phi$.

Exercise E130

Consider the following mapping:

$$\begin{aligned}\phi : (L, \times) &\longrightarrow (\mathbb{R}^*, \times)\\ \begin{pmatrix} a & 0 \\ c & d \end{pmatrix} &\longmapsto ad.\end{aligned}$$

(This mapping ϕ maps each matrix in L to its determinant.)

(a) Show that ϕ is a homomorphism.

(b) Find $\operatorname{Im}\phi$ and $\operatorname{Ker}\phi$.

(c) State a standard group isomorphic to the quotient group $L/\operatorname{Ker}\phi$.

In each of Worked Exercise E51 and Exercises E129 and E130, we found a standard group isomorphic to a quotient group $G/\operatorname{Ker}\phi$ by finding $\operatorname{Im}\phi$ and then using the fact that $G/\operatorname{Ker}\phi \cong \operatorname{Im}\phi$, by the First Isomorphism Theorem. In these cases, this gave us an immediate answer because $\operatorname{Im}\phi$ *was itself* a standard group.

When $\operatorname{Im}\phi$ is not a standard group, we may still be able to find a standard group isomorphic to $G/\operatorname{Ker}\phi$ by finding a standard group isomorphic to $\operatorname{Im}\phi$; this group will then, in turn, be isomorphic to $G/\operatorname{Ker}\phi$. This is illustrated in the next worked exercise and in the exercise that follows it.

Worked Exercise E52

Consider the following mapping:

$$\phi : (L, \times) \longrightarrow (L, \times)$$
$$\begin{pmatrix} a & 0 \\ c & d \end{pmatrix} \longmapsto \begin{pmatrix} 1 & 0 \\ 0 & d^2 \end{pmatrix}.$$

You saw that this mapping is a homomorphism in Worked Exercise E44 in Subsection 1.2, and in Exercise E123 in Subsection 2.3 you saw that its image and kernel are

$$\operatorname{Im}\phi = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & r \end{pmatrix} : r \in \mathbb{R}^+ \right\}$$

and

$$\operatorname{Ker}\phi = \left\{ \begin{pmatrix} a & 0 \\ c & \pm 1 \end{pmatrix} : a, c \in \mathbb{R},\ a \neq 0 \right\}.$$

Find a standard group isomorphic to the quotient group $L/\operatorname{Ker}\phi$.

Solution

By the First Isomorphism Theorem, the quotient group $L/\operatorname{Ker}\phi$ is isomorphic to $\operatorname{Im}\phi$.

Here $\operatorname{Im}\phi$, given in the question, is not a standard group. We guess that $\operatorname{Im}\phi \cong (\mathbb{R}^+, \times)$ by considering the expression for $\operatorname{Im}\phi$.

We now show that $\operatorname{Im}\phi$ is isomorphic to $(\mathbb{R}^+, \times)$.

To do this, we show that there is an isomorphism, say θ, from $\operatorname{Im}\phi$ to $(\mathbb{R}^+, \times)$.

Consider the mapping

$$\theta : \operatorname{Im}\phi \longrightarrow \mathbb{R}^+$$
$$\begin{pmatrix} 1 & 0 \\ 0 & r \end{pmatrix} \longmapsto r.$$

This mapping is one-to-one, because if

$$\mathbf{A} = \begin{pmatrix} 1 & 0 \\ 0 & r \end{pmatrix} \quad \text{and} \quad \mathbf{B} = \begin{pmatrix} 1 & 0 \\ 0 & s \end{pmatrix}$$

are elements of $\operatorname{Im}\phi$ such that $\theta(\mathbf{A}) = \theta(\mathbf{B})$, then $r = s$ by the definition of θ and hence $\mathbf{A} = \mathbf{B}$.

It is also onto, because if $r \in \mathbb{R}^+$ then r is the image under θ of the element

$$\begin{pmatrix} 1 & 0 \\ 0 & r \end{pmatrix}$$

of $\operatorname{Im}\phi$.

Finally, θ has the homomorphism property because, for all $r, s \in \mathbb{R}^+$,

$$\begin{aligned} \theta\left(\begin{pmatrix} 1 & 0 \\ 0 & r \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & s \end{pmatrix}\right) &= \theta\begin{pmatrix} 1 & 0 \\ 0 & rs \end{pmatrix} \\ &= rs \\ &= \theta\begin{pmatrix} 1 & 0 \\ 0 & r \end{pmatrix}\theta\begin{pmatrix} 1 & 0 \\ 0 & s \end{pmatrix}. \end{aligned}$$

Thus θ is an isomorphism, so

$$L/\operatorname{Ker}\phi \cong \operatorname{Im}\phi \cong (\mathbb{R}^+, \times).$$

So a standard group isomorphic to $L/\operatorname{Ker}\phi$ is $(\mathbb{R}^+, \times)$.

Exercise E131

Consider the following mapping:

$$\phi : (L, \times) \longrightarrow (L, \times)$$
$$\begin{pmatrix} a & 0 \\ c & d \end{pmatrix} \longmapsto \begin{pmatrix} 1/a & 0 \\ 0 & 1 \end{pmatrix}.$$

(a) Show that ϕ is a homomorphism.

(b) Find $\operatorname{Im}\phi$ and $\operatorname{Ker}\phi$.

(c) Find a standard group that is isomorphic to the quotient group $L/\operatorname{Ker}\phi$.

The First Isomorphism Theorem has the following interesting corollary for *finite* groups.

Corollary E56

Let $(G, \circ)$ be a finite group and let $\phi : (G, \circ) \longrightarrow (H, *)$ be a homomorphism. Then

$$|\operatorname{Ker}\phi| \times |\operatorname{Im}\phi| = |G|.$$

Proof Since G is finite, each coset of $\operatorname{Ker}\phi$ in G contains the same number of elements as $\operatorname{Ker}\phi$, and hence the order of $G/\operatorname{Ker}\phi$ is

$$\frac{|G|}{|\operatorname{Ker}\phi|}.$$

It follows from the First Isomorphism Theorem that the order of $G/\operatorname{Ker}\phi$ is the same as the order of $\operatorname{Im}\phi$. Hence

$$\frac{|G|}{|\operatorname{Ker}\phi|} = |\operatorname{Im}\phi|.$$

Rearranging this equation gives the equation in the statement of the corollary. ■

If $(G, \circ)$ and $(H, *)$ are finite groups, then the following numerical relationships hold for any homomorphism $\phi : (G, \circ) \longrightarrow (H, *)$:

$|\operatorname{Ker}(\phi)|$ divides $|G|$ (by Lagrange's Theorem),

$|\operatorname{Im}(\phi)|$ divides $|H|$ (by Lagrange's Theorem),

$|\operatorname{Im}(\phi)|$ divides $|G|$ (by Corollary E56).

In particular, the order of $\operatorname{Im}\phi$ is a common factor of the orders of the domain group $(G, \circ)$ and the codomain group $(H, *)$.

Worked Exercise E53

Prove that the only homomorphism from A_4 (the alternating group of degree 4) to $(\mathbb{Z}_7, +_7)$ is the trivial one.

Solution

Let $\phi : A_4 \longrightarrow \mathbb{Z}_7$ be a homomorphism. By Corollary E56 and Lagrange's Theorem, the order of $\operatorname{Im}\phi$ divides the orders of A_4 and $\mathbb{Z}_7$, which are 12 and 7, respectively. But 12 and 7 have greatest common factor 1, so the order of $\operatorname{Im}\phi$ is 1. Hence, since $\operatorname{Im}\phi$ is a subgroup of $(\mathbb{Z}_7, +_7)$, we have $\operatorname{Im}\phi = \{0\}$. Therefore ϕ is the trivial homomorphism

$$\begin{aligned} \phi : A_4 &\longrightarrow \mathbb{Z}_7 \\ f &\longmapsto 0. \end{aligned}$$

Exercise E132

(a) Prove that the only homomorphism from $(\mathbb{Z}_{11}, +_{11})$ to S_3 is the trivial one.

(b) Prove that the only homomorphism from $S(\triangle)$ to $(\mathbb{Z}_3, +_3)$ is the trivial one.

Hint: You were asked to find the normal subgroups of $S(\triangle)$ in Exercise E39 in Subsection 3.3 of Unit E2.

Bartel van der Waerden

The first time the First, Second and Third Isomorphism Theorems appeared explicitly in the context of groups was in the famous two-volume book on abstract algebra by Bartel van der Waerden (1903–1996), *Moderne Algebra*. This book was first published in 1930–1, with an English translation appearing in 1949–50, and was originally based on lectures given by Emile Artin (1898–1962) and Emmy Noether (1882–1935). Noether, who is often described as the most important woman mathematician in the history of mathematics for her work on abstract algebra and theoretical physics, had earlier published the three theorems in a slightly different context in a paper in *Mathematische Annalen* in 1927.

Emmy Noether

3.3 Infinite quotient groups of domain groups by kernels (optional)

In the previous subsection we considered some quotient groups of the form $G/\operatorname{Ker}\phi$, where $\phi : (G, \circ) \longrightarrow (H, *)$ is a homomorphism. We used the First Isomorphism Theorem to find standard groups isomorphic to these quotient groups.

In this final, optional, subsection of the unit we will look in detail at two of these quotient groups, finding their elements and considering their binary operations. These two quotient groups are further examples of *infinite* quotient groups: so far in the module you have looked in detail at just one such quotient group, namely $\mathbb{R}/\mathbb{Z}$, which you met in Subsection 1.2 of Unit E2. (An infinite quotient group of an infinite group of matrices was also mentioned briefly at the end of Unit E2.)

The two examples that we will look at in this subsection are those from Worked Exercise E51 and Exercise E129 in the previous subsection. In the first of these examples the domain group G of the homomorphism ϕ is $(\mathbb{C}^*, \times)$, and in the second it is $(\mathbb{R}^2, +)$. So in each case the domain group G has a geometric interpretation, and hence the elements of the quotient group $G/\operatorname{Ker}\phi$, which are subsets of G, also have geometric interpretations.

Worked Exercise E54

Consider the homomorphism

$$\begin{aligned}\phi : (\mathbb{C}^*, \times) &\longrightarrow (\mathbb{R}^*, \times)\\ z &\longmapsto |z|.\end{aligned}$$

(You saw that this mapping is a homomorphism in Worked Exercise E41 in Subsection 1.2.)

In Worked Exercise E47 in Subsection 2.3 we found that its kernel is

$$\operatorname{Ker}\phi = \{z \in \mathbb{C} : |z| = 1\}.$$

That is, its kernel is the unit circle in the complex plane (the circle with centre 0 and radius 1), as shown in Figure 29.

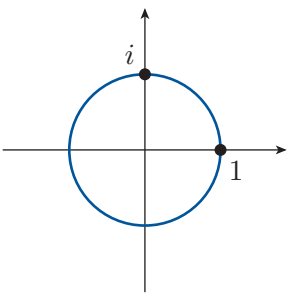

Figure 29 The unit circle in the complex plane

(a) Find the particular cosets $2\operatorname{Ker}\phi$ and $3i\operatorname{Ker}\phi$ and describe them geometrically.

(b) Find the general coset $a\operatorname{Ker}\phi$, where $a \in \mathbb{C}^*$, and describe it geometrically.

(c) Hence specify the elements of the quotient group $\mathbb{C}^*/\operatorname{Ker}\phi$, and describe them geometrically.

Solution

(a) The coset $2\operatorname{Ker}\phi$ is obtained by multiplying each element of $\operatorname{Ker}\phi$ by 2.

We have

$$2\operatorname{Ker}\phi = \{2z : z \in \operatorname{Ker}\phi\}$$

Since $\operatorname{Ker}\phi$ consists of all the complex numbers with modulus 1, we can see from this specification of the coset $2\operatorname{Ker}\phi$ that it will consist of all the complex numbers with modulus 2. We can also prove this algebraically, as below. The specification of $\operatorname{Ker}\phi$, given in the question, tells us that the condition $z \in \operatorname{Ker}\phi$ is equivalent to the conditions $z \in \mathbb{C}$, $|z| = 1$.

$$= \{2z : z \in \mathbb{C},\ |z| = 1\}$$

To obtain z rather than $2z$ in front of the colon, replace $2z$ by z everywhere.

$$= \{z : z/2 \in \mathbb{C},\ |z/2| = 1\}$$

Simplify both conditions. The condition $z/2 \in \mathbb{C}$ says the same as $z \in \mathbb{C}$.

$$\begin{aligned}&= \{z : z \in \mathbb{C},\ |z|/|2| = 1\}\\ &= \{z : z \in \mathbb{C},\ |z| = 2\}\end{aligned}$$

We can write '$\{z : z \in \mathbb{C}, \ldots\}$' more simply as '$\{z \in \mathbb{C} : \ldots\}$'.

$$= \{z \in \mathbb{C} : |z| = 2\}.$$

This is the circle with centre 0 and radius 2 in the complex plane.

Similarly,

$$\begin{aligned} 3i \operatorname{Ker}\phi &= \{3iz : z \in \operatorname{Ker}\phi\} \\ &= \{3iz : z \in \mathbb{C},\ |z| = 1\} \\ &= \{z : z/(3i) \in \mathbb{C},\ |z/(3i)| = 1\} \\ &= \{z : z \in \mathbb{C},\ |z|/|3i| = 1\} \\ &= \{z \in \mathbb{C} : |z| = 3\}. \end{aligned}$$

This is the circle with centre 0 and radius 3 in the complex plane.

(b) For any $a \in \mathbb{C}^*$,

$$\begin{aligned} a \operatorname{Ker}\phi &= \{az : z \in \operatorname{Ker}\phi\} \\ &= \{az : z \in \mathbb{C},\ |z| = 1\} \\ &= \{z : z/a \in \mathbb{C},\ |z/a| = 1\} \\ &= \{z : z \in \mathbb{C},\ |z|/|a| = 1\} \\ &= \{z \in \mathbb{C} : |z| = |a|\}. \end{aligned}$$

This is the circle with centre 0 and radius $|a|$ in the complex plane.

(c) The elements of the quotient group $\mathbb{C}^*/\operatorname{Ker}\phi$ are the sets of the form

$$\{z \in \mathbb{C} : |z| = r\}$$

where $r \in \mathbb{R}^+$.

That is, they are the circles with centre 0 and positive radius in the complex plane (the complex number 0 itself is not one of these circles). (Some of these circles are shown in Figure 30.)

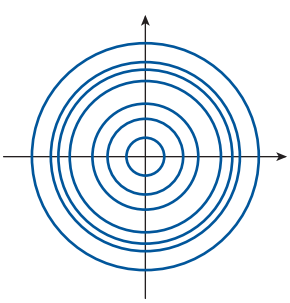

Figure 30 Circles with centre 0 in the complex plane

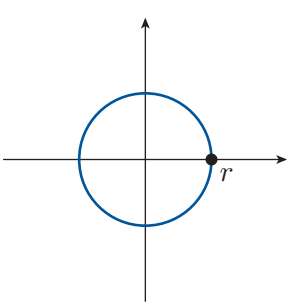

Figure 31 The circle with centre 0 and radius r contains the complex number r

We can describe the binary operation of the quotient group in Worked Exercise E54 in terms of the circles that are its elements. The circle with centre 0 and positive radius r is the coset of $\operatorname{Ker}\phi$ containing the number r (which is an element of $\mathbb{C}^*$, as shown in Figure 31), so it can be denoted by

$$r \operatorname{Ker}\phi.$$

The rule for set composition of such cosets is (by Theorem E1 in Unit E2)

$$r \operatorname{Ker}\phi \cdot s \operatorname{Ker}\phi = (rs) \operatorname{Ker}\phi,$$

where $r, s \in \mathbb{R}^+$. That is, the binary operation of the quotient group $\mathbb{C}^*/\operatorname{Ker}\phi$ has the rule

$$(\text{circle of radius } r) \cdot (\text{circle of radius } s) = (\text{circle of radius } rs),$$

for all $r, s \in \mathbb{R}^+$.

So the quotient group $\mathbb{C}^*/\operatorname{Ker}\phi$ in Worked Exercise E54 is the group of all circles with centre 0 and positive radius in the complex plane under this binary operation.

The elements of this group and the definition of its binary operation appear to indicate that it is isomorphic to the group $(\mathbb{R}^+, \times)$, and indeed this is what was found using the First Isomorphism Theorem in the solution to Worked Exercise E51 in the previous subsection.

Exercise E133

Consider the homomorphism

$$\begin{aligned}\phi : (\mathbb{R}^2, +) &\longrightarrow (\mathbb{R}, +)\\ (x, y) &\longmapsto x + y.\end{aligned}$$

You saw that this mapping is a homomorphism in Exercise E129 in Subsection 3.2. You also saw there that its kernel is

$$\operatorname{Ker}\phi = \{(x, y) \in \mathbb{R}^2 : y = -x\}.$$

This is the line $y = -x$ in $\mathbb{R}^2$, that is, the line through the origin with gradient -1.

(Alternatively we can write $\operatorname{Ker}\phi$ as

$$\operatorname{Ker}\phi = \{(k, -k) : k \in \mathbb{R}\}.)$$

(a) Find the particular coset $(2, 3) + \operatorname{Ker}\phi$ and describe it geometrically.

(b) Find the general coset $(a, b) + \operatorname{Ker}\phi$, where $(a, b) \in \mathbb{R}^2$, and describe it geometrically.

(c) Hence specify the elements of the quotient group $\mathbb{R}^2/\operatorname{Ker}\phi$ and describe them geometrically.

As for the quotient group in Worked Exercise E54, we can describe the binary operation of the quotient group in Exercise E133 in terms of the geometric interpretation of its elements. You should have found that the elements of the quotient group $\mathbb{R}^2/\operatorname{Ker}\phi$ in Exercise E133 are the lines in the plane with gradient -1.

The rule for set composition of these elements is (by Theorem E1 in Unit E2)

$$\big((0, c) + \operatorname{Ker}\phi\big) + \big((0, d) + \operatorname{Ker}\phi\big) = \big((0, c) + (0, d)\big) + \operatorname{Ker}\phi,$$

that is,

$$\big((0, c) + \operatorname{Ker}\phi\big) + \big((0, d) + \operatorname{Ker}\phi\big) = (0, c + d) + \operatorname{Ker}\phi.$$

We can express this rule as

$$(\text{line } y = -x + c) + (\text{line } y = -x + d) = (\text{line } y = -x + (c + d)).$$

So the quotient group $\mathbb{R}^2/\operatorname{Ker}\phi$ in Exercise E133 is the group of lines in the plane with gradient -1 under this binary operation.

The elements of this group and the definition of its binary operation appear to indicate that it is isomorphic to the group $(\mathbb{R}, +)$, and indeed this is what was found using the First Isomorphism Theorem in the solution to Exercise E129 in the previous subsection.

Summary

In this unit you have met the idea of a *homomorphism* from a group to a group, and considered many examples. You have seen that homomorphisms preserve important features of the structure of the domain group, including composites, the identity, inverses, powers and conjugates. You have studied the *image* and *kernel* of a homomorphism, and explored some of the properties of these sets, such as the fact that they are always groups themselves. You have also learned that kernels of homomorphisms and normal subgroups are in fact the same objects. You have seen that a linear transformation is a special type of homomorphism, and met several parallels between homomorphisms in group theory and linear transformations in linear algebra. Finally you met the *First Isomorphism Theorem*, which links homomorphisms and quotient groups.

Learning outcomes

After working through this unit, you should be able to:

- explain what is meant by a *homomorphism*
- understand that an isomorphism is a special case of a homomorphism
- check whether a mapping between groups is a homomorphism, or an isomorphism, or neither
- understand that a homomorphism preserves composites, the identity, inverses, powers, conjugates and the properties of being abelian and being cyclic
- understand what are meant by the *image* and *kernel* of a homomorphism
- understand that the image of a homomorphism is a subgroup of the codomain group, and the kernel of a homomorphism is a normal subgroup of the domain group
- know that a homomorphism is one-to-one if and only if its kernel contains the identity element of the domain group alone
- understand that all the elements in a coset of the kernel of a homomorphism have the same image under the homomorphism
- understand that, for any homomorphism, the quotient group formed by the cosets of the kernel is isomorphic to the image group (the *First Isomorphism Theorem*).

Solutions to exercises

Solution to Exercise E99

(a) As mentioned in the question, the given group tables (repeated here for convenience) have the same pattern:

$\circ$	e	a	r	s
e	e	a	r	s
a	a	e	s	r
r	r	s	e	a
s	s	r	a	e

$(S(\square), \circ)$

$\times_{12}$	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

$(U_{12}, \times_{12})$

So the following mapping ϕ_1, obtained by matching up the row (or column) labels in order, is an isomorphism.

$$\begin{aligned} \phi_1 : (S(\square), \circ) &\longrightarrow (U_{12}, \times_{12}) \\ e &\longmapsto 1 \\ a &\longmapsto 5 \\ r &\longmapsto 7 \\ s &\longmapsto 11 \end{aligned}$$

Now consider the following mappings ϕ_2 and ϕ_3.

$$\begin{aligned} \phi_2 : (S(\square), \circ) &\longrightarrow (U_{12}, \times_{12}) \\ e &\longmapsto 1 \\ a &\longmapsto 5 \\ r &\longmapsto 11 \\ s &\longmapsto 7 \end{aligned}$$

$$\begin{aligned} \phi_3 : (S(\square), \circ) &\longrightarrow (U_{12}, \times_{12}) \\ e &\longmapsto 1 \\ a &\longmapsto 7 \\ r &\longmapsto 5 \\ s &\longmapsto 11 \end{aligned}$$

Replacing each entry in the group table of $(S(\square), \circ)$ above by its image under ϕ_2 and its image under ϕ_3, respectively, gives the following tables.

	1	5	11	7
1	1	5	11	7
5	5	1	7	11
11	11	7	1	5
7	7	11	5	1

	1	7	5	11
1	1	7	5	11
7	7	1	11	5
5	5	11	1	7
11	11	5	7	1

Each of these tables is a correct group table for $(U_{12}, \times_{12})$ (because, for each table, each cell in the body of the table contains the result of combining the row label of the cell with the column label of the cell). So both ϕ_2 and ϕ_3 are isomorphisms.

(In fact there are six different isomorphisms from $(S(\square), \circ)$ to $(U_{12}, \times_{12})$: any one-to-one and onto mapping from $(S(\square), \circ)$ to $(U_{12}, \times_{12})$ that maps the identity element e of $(S(\square), \circ)$ to the identity element 1 of $(U_{12}, \times_{12})$ is an isomorphism.)

(b) Consider the following one-to-one and onto mapping ϕ_4 from $(S(\square), \circ)$ to $(U_{12}, \times_{12})$.

$$\begin{aligned} \phi_4 : (S(\square), \circ) &\longrightarrow (U_{12}, \times_{12}) \\ e &\longmapsto 5 \\ a &\longmapsto 1 \\ r &\longmapsto 7 \\ s &\longmapsto 11 \end{aligned}$$

Replacing each entry in the group table of $S(\square)$ above by its image under ϕ_4 gives the following table.

	5	1	7	11
5	5	1	7	11
1	1	5	11	7
7	7	11	5	1
11	11	7	1	5

This is not a group table of $(U_{12}, \times_{12})$ because, for example, it is not true that $5 \times_{12} 5 = 5$.

Hence ϕ_4 is an example of a one-to-one and onto mapping from $(S(\square), \circ)$ to $(U_{12}, \times_{12})$ that is not an isomorphism.

(There are other possible answers here: any one-to-one and onto mapping from $(S(\square), \circ)$ to $(U_{12}, \times_{12})$ that does *not* map e to 1 will do.)

Solution to Exercise E100

The given group table for $(S^+(\square), \circ)$ is as follows. (It is repeated here for convenience.)

$\circ$	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

Consider the following one-to-one and onto mapping from $(S^+(\square), \circ)$ to $(U_{10}, \times_{10})$.

$$\begin{aligned} \phi : (S^+(\square), \circ) &\longrightarrow (U_{10}, \times_{10}) \\ e &\longmapsto 1 \\ a &\longmapsto 3 \\ b &\longmapsto 7 \\ c &\longmapsto 9 \end{aligned}$$

Replacing each entry in the group table of $(S^+(\square), \circ)$ above by its image under ϕ gives the following table.

	1	3	7	9
1	1	3	7	9
3	3	7	9	1
7	7	9	1	3
9	9	1	3	7

This is not a group table of $(U_{10}, \times_{10})$ because, for example, it is not true that $3 \times_{10} 3 = 7$.

Hence ϕ is an example of a one-to-one and onto mapping from $(S^+(\square), \circ)$ to $(U_{10}, \times_{10})$ that maps the identity element of $(S^+(\square), \circ)$ to the identity element of $(U_{10}, \times_{10})$ but is not an isomorphism.

(There are other possible answers here: any one-to-one and onto mapping from $(S^+(\square), \circ)$ to $(U_{10}, \times_{10})$ that maps e to 1 but does not map b (the only element of order 2 in $(S^+(\square), \circ)$) to 9 (the only element of order 2 in $(U_{10}, \times_{10})$) will do. There are three such mappings other than the one above, as follows.

$$\begin{aligned} \phi : (S^+(\square), \circ) &\longrightarrow (U_{10}, \times_{10}) \\ e &\longmapsto 1 \\ a &\longmapsto 7 \\ b &\longmapsto 3 \\ c &\longmapsto 9 \end{aligned}$$

$$\begin{aligned} \phi : (S^+(\square), \circ) &\longrightarrow (U_{10}, \times_{10}) \\ e &\longmapsto 1 \\ a &\longmapsto 9 \\ b &\longmapsto 3 \\ c &\longmapsto 7 \end{aligned}$$

$$\begin{aligned} \phi : (S^+(\square), \circ) &\longrightarrow (U_{10}, \times_{10}) \\ e &\longmapsto 1 \\ a &\longmapsto 9 \\ b &\longmapsto 7 \\ c &\longmapsto 3) \end{aligned}$$

Solution to Exercise E101

The group table of $(S(\square), \circ)$ is as follows. (It is repeated here for convenience.)

$\circ$	e	a	r	s
e	e	a	r	s
a	a	e	s	r
r	r	s	e	a
s	s	r	a	e

The following mapping ϕ_1 maps every element of $(S(\square), \circ)$ to itself, so it is an isomorphism and hence an automorphism.

$$\begin{aligned} \phi_1 : (S(\square), \circ) &\longrightarrow (S(\square), \circ) \\ e &\longmapsto e \\ a &\longmapsto a \\ r &\longmapsto r \\ s &\longmapsto s \end{aligned}$$

Now consider the following mapping ϕ_2.

$$\begin{aligned} \phi_2 : (S(\square), \circ) &\longrightarrow (S(\square), \circ) \\ e &\longmapsto e \\ a &\longmapsto r \\ r &\longmapsto a \\ s &\longmapsto s \end{aligned}$$

Replacing each entry in the group table of $(S(\square), \circ)$ above by its image under ϕ_2 gives the following table.

	e	r	a	s
e	e	r	a	s
r	r	e	s	a
a	a	s	e	r
s	s	a	r	e

This table is a correct group table for $(S(\square), \circ)$, so ϕ_2 is an isomorphism and hence an automorphism.

(There are six different automorphisms of $(S(\square), \circ)$: any one-to-one and onto mapping from $(S(\square), \circ)$ to itself that maps e to itself will do.)

Solution to Exercise E102

The mapping ϕ (the exponential function) is one-to-one.

It is also onto, because its image set is $(0, \infty) = \mathbb{R}^+$.

We now check that ϕ preserves composites. Let $x, y \in \mathbb{R}$. We have to show that

$$\phi(x + y) = \phi(x) \times \phi(y),$$

that is,

$$e^{x+y} = e^x \times e^y.$$

This is true by the index laws for $\mathbb{R}$, so ϕ preserves composites.

Hence ϕ is an isomorphism.

Solution to Exercise E103

To show that ϕ is one-to-one, suppose that m and n are elements of $\mathbb{Z}$ such that

$$\phi(m) = \phi(n).$$

Then

$$-m = -n,$$

which gives

$$m = n.$$

Thus ϕ is one-to-one.

Also, ϕ is onto, because each element n of the codomain group $(\mathbb{Z}, +)$ is the image under ϕ of the element $-n$ of the domain group $(\mathbb{Z}, +)$.

We now check that ϕ preserves composites. Let $m, n \in \mathbb{Z}$. We have to show that

$$\phi(m + n) = \phi(m) + \phi(n).$$

Now

$$\begin{aligned} \phi(m + n) &= -(m + n) \\ &= (-m) + (-n) \\ &= \phi(m) + \phi(n). \end{aligned}$$

Thus ϕ preserves composites.

Hence ϕ is an isomorphism.

Solution to Exercise E104

(a) This mapping ϕ is not one-to-one. For example, $\phi(i) = \phi(1) = 1$.

(This mapping ϕ is onto and preserves composites.)

(b) This mapping ϕ is not onto. For example, the element 1 of the codomain is not the image under ϕ of any element of the domain.

(This mapping ϕ is one-to-one and preserves composites.)

(c) This mapping ϕ is not onto, because $2^x > 0$ for all $x \in \mathbb{R}$, so, for example, the element -1 of the codomain is not the image under ϕ of any element of the domain.

In fact, this mapping ϕ does not preserve composites either as, in general, $2^{x \times y} \neq 2^x \times 2^y$. For example,

$$\phi(1 \times 2) = 2^{1 \times 2} = 2^2 = 4$$

whereas

$$\phi(1) \times \phi(2) = 2^1 \times 2^2 = 2 \times 4 = 8.$$

(This mapping ϕ is one-to-one.)

Solution to Exercise E105

The group $(\mathbb{Z}_{10}, +_{10})$ is a cyclic group of order 10, generated by 1. In this group the consecutive multiples of the generator 1 starting from the identity 0 are

$$0, 1, 2, 3, 4, 5, 6, 7, 8, 9, \ldots.$$

We try to find a generator of the group $(\mathbb{Z}_{11}^*, \times_{11})$. In $(\mathbb{Z}_{11}^*, \times_{11})$ the consecutive powers of 2 starting from 2^0 are

$$1, 2, 4, 8, 5, 10, 9, 7, 3, 6, \ldots.$$

All the elements of $\mathbb{Z}_{11}^*$ appear in this list, so 2 is a generator of $(\mathbb{Z}_{11}^*, \times_{11})$.

Matching each multiple of the generator 1 of $(\mathbb{Z}_{10}, +_{10})$ to the corresponding power of the generator 2 of $(\mathbb{Z}_{11}^*, \times_{11})$ gives the following isomorphism:

$$\begin{aligned}\phi : (\mathbb{Z}_{10}, +_{10}) &\longrightarrow (\mathbb{Z}_{11}^*, \times_{11})\\ 0 &\longmapsto 1\\ 1 &\longmapsto 2\\ 2 &\longmapsto 4\\ 3 &\longmapsto 8\\ 4 &\longmapsto 5\\ 5 &\longmapsto 10\\ 6 &\longmapsto 9\\ 7 &\longmapsto 7\\ 8 &\longmapsto 3\\ 9 &\longmapsto 6.\end{aligned}$$

(There are alternative answers, as follows, since 6, 7 and 8 are also generators of $(\mathbb{Z}_{11}^*, \times_{11})$:

$$\begin{array}{lll} 0 \longmapsto 1 & 0 \longmapsto 1 & 0 \longmapsto 1\\ 1 \longmapsto 6 & 1 \longmapsto 7 & 1 \longmapsto 8\\ 2 \longmapsto 3 & 2 \longmapsto 5 & 2 \longmapsto 9\\ 3 \longmapsto 7 & 3 \longmapsto 2 & 3 \longmapsto 6\\ 4 \longmapsto 9 & 4 \longmapsto 3 & 4 \longmapsto 4\\ 5 \longmapsto 10 & 5 \longmapsto 10 & 5 \longmapsto 10\\ 6 \longmapsto 5 & 6 \longmapsto 4 & 6 \longmapsto 3\\ 7 \longmapsto 8 & 7 \longmapsto 6 & 7 \longmapsto 2\\ 8 \longmapsto 4 & 8 \longmapsto 9 & 8 \longmapsto 5\\ 9 \longmapsto 2 & 9 \longmapsto 8 & 9 \longmapsto 7.)\end{array}$$

Solution to Exercise E106

In the group $(\mathbb{Z}_4, +_4)$ the consecutive multiples of the generator 1 starting from the identity 0 are

$$0, 1, 2, 3, \ldots.$$

In the group $(\mathbb{Z}_8, +_8)$ the consecutive multiples of 2 starting from the identity 0 are

$$0, 2, 4, 6, \ldots.$$

Thus the cyclic subgroup of $(\mathbb{Z}_8, +_8)$ generated by 2 is $\langle 2 \rangle = \{0, 2, 4, 6\}$.

Matching each multiple of the generator 1 of $(\mathbb{Z}_4, +_4)$ to the corresponding multiple of the generator 2 of the subgroup $\langle 2 \rangle$ of $(\mathbb{Z}_8, +_8)$ gives the following isomorphism:

$$\begin{aligned}\phi : (\mathbb{Z}_4, +_4) &\longrightarrow (\{0, 2, 4, 6\}, +_4)\\ 0 &\longmapsto 0\\ 1 &\longmapsto 2\\ 2 &\longmapsto 4\\ 3 &\longmapsto 6.\end{aligned}$$

(The subgroup of $(\mathbb{Z}_8, +_8)$ generated by 2 is also generated by 6, so an alternative answer is

$$\begin{aligned}\phi : (\mathbb{Z}_4, +_4) &\longrightarrow (\{0, 2, 4, 6\}, +_4)\\ 0 &\longmapsto 0\\ 1 &\longmapsto 6\\ 2 &\longmapsto 4\\ 3 &\longmapsto 2.)\end{aligned}$$

Solution to Exercise E107

(a) The homomorphism property for ϕ is

$$\phi(x \times y) = \phi(x) \times \phi(y) \quad \text{for all } x, y \in \mathbb{R}^*.$$

We check whether it holds. Let $x, y \in \mathbb{R}^*$. Then

$$\begin{aligned}\phi(x \times y) &= (x \times y)^2\\ &= x^2 \times y^2\\ &= \phi(x) \times \phi(y).\end{aligned}$$

Thus ϕ is a homomorphism.

(b) The homomorphism property for ϕ is

$$\phi(m + n) = \phi(m) + \phi(n) \quad \text{for all } m, n \in \mathbb{Z}.$$

The mapping ϕ does not have this property, since, for example, $1 \in \mathbb{Z}$ and

$$\phi(1 + 1) = \phi(2) = 2^2 = 4,$$

whereas

$$\phi(1) + \phi(1) = 1^2 + 1^2 = 1 + 1 = 2,$$

so $\phi(1 + 1) \neq \phi(1) + \phi(1)$. Hence ϕ is not a homomorphism.

(c) The homomorphism property for ϕ is

$$\phi(m +_6 n) = \phi(m) +_6 \phi(n) \quad \text{for all } m, n \in \mathbb{Z}_6.$$

We check whether it holds. Let $m, n \in \mathbb{Z}_6$. Then

$$\begin{aligned}\phi(m +_6 n) &= 3 \times_6 (m +_6 n)\\ &= (3 \times_6 m) +_6 (3 \times_6 n)\end{aligned}$$

(by the distributive law for modular arithmetic)

$$= \phi(m) +_6 \phi(n).$$

Thus ϕ is a homomorphism.

(d) The homomorphism property for ϕ is

$$\phi(m + n) = \phi(m) \times \phi(n) \quad \text{for all } m, n \in \mathbb{Z}.$$

We check whether it holds. Let $m, n \in \mathbb{Z}$. Then

$$\begin{aligned}\phi(m + n) &= 2^{m+n}\\ &= 2^m \times 2^n\\ &= \phi(m) \times \phi(n).\end{aligned}$$

Thus ϕ is a homomorphism.

(e) The homomorphism property for ϕ is

$$\phi(x + y) = \phi(x) +_2 \phi(y) \quad \text{for all } x, y \in \mathbb{R}.$$

The mapping ϕ does not have this property, since, for example, $\pi \in \mathbb{R}$ and

$$\phi(\pi + \pi) = \phi(2\pi) = 1$$

whereas

$$\phi(\pi) +_2 \phi(\pi) = 1 +_2 1 = 0.$$

So $\phi(\pi + \pi) \neq \phi(\pi) +_2 \phi(\pi)$. Hence ϕ is not a homomorphism.

(The number 2π is irrational, because if 2π were rational then $\pi = (2\pi)/2$ would be rational.)

(f) The homomorphism property for ϕ is

$$\phi((x_1, y_1) + (x_2, y_2)) = \phi(x_1, y_1) + \phi(x_2, y_2)$$
$$\text{for all } (x_1, y_1), (x_2, y_2) \in \mathbb{R}^2.$$

We check whether it holds. Let $(x_1, y_1), (x_2, y_2) \in \mathbb{R}^2$.

The left-hand side of the homomorphism property equation is

$$\begin{aligned}&\phi((x_1, y_1) + (x_2, y_2))\\ &= \phi(x_1 + x_2, y_1 + y_2)\\ &= (2(x_1 + x_2) - (y_1 + y_2),\ 6(x_1 + x_2) - 3(y_1 + y_2))\\ &= (2x_1 + 2x_2 - y_1 - y_2,\ 6x_1 + 6x_2 - 3y_1 - 3y_2).\end{aligned}$$

The right-hand side is

$$\begin{aligned}&\phi(x_1, y_1) + \phi(x_2, y_2)\\ &= (2x_1 - y_1, 6x_1 - 3y_1) + (2x_2 - y_2, 6x_2 - 3y_2)\\ &= (2x_1 + 2x_2 - y_1 - y_2,\ 6x_1 + 6x_2 - 3y_1 - 3y_2).\end{aligned}$$

Since the two sides are equal, ϕ is a homomorphism.

(In fact, as you will see later in this subsection, there is a shortcut way to confirm that this mapping is a homomorphism, using the fact that it is a linear transformation from the vector space $\mathbb{R}^2$ to itself.)

(For simplicity, we write $\phi(x, y)$ for $\phi((x, y))$, as in Unit C3 *Linear transformations*.)

Solution to Exercise E108

Let $f, g \in S_n$. We have to show that

$$\phi(f \circ g) = \phi(f) +_2 \phi(g).$$

We know that a composite of two even permutations or two odd permutations is even, and a composite of a even permutation and an odd permutation is odd. Thus we have the following.

If f is even and g is even then $f \circ g$ is even so

$$\phi(f \circ g) = 0 \quad \text{and} \quad \phi(f) +_2 \phi(g) = 0 +_2 0 = 0.$$

If f is even and g is odd then $f \circ g$ is odd so

$$\phi(f \circ g) = 1 \quad \text{and} \quad \phi(f) +_2 \phi(g) = 0 +_2 1 = 1.$$

If f is odd and g is even then $f \circ g$ is odd so

$$\phi(f \circ g) = 1 \quad \text{and} \quad \phi(f) +_2 \phi(g) = 1 +_2 0 = 1.$$

If f is odd and g is odd then $f \circ g$ is even so

$$\phi(f \circ g) = 0 \quad \text{and} \quad \phi(f) +_2 \phi(g) = 1 +_2 1 = 0.$$

Thus in all cases $\phi(f \circ g) = \phi(f) +_2 \phi(g)$. Hence ϕ is a homomorphism.

Solution to Exercise E109

(a) Let $\mathbf{A}, \mathbf{B} \in L$. We have to show that

$$\phi(\mathbf{AB}) = \phi(\mathbf{A})\phi(\mathbf{B}).$$

Now

$$\mathbf{A} = \begin{pmatrix} r & 0 \\ t & u \end{pmatrix} \quad \text{and} \quad \mathbf{B} = \begin{pmatrix} v & 0 \\ x & y \end{pmatrix},$$

for some $r, t, u, v, x, y \in \mathbb{R}$ with $ru \neq 0$ and $vy \neq 0$. Hence

$$\begin{aligned} \phi(\mathbf{AB}) &= \phi\left(\begin{pmatrix} r & 0 \\ t & u \end{pmatrix}\begin{pmatrix} v & 0 \\ x & y \end{pmatrix}\right) \\ &= \phi\begin{pmatrix} rv & 0 \\ tv + ux & uy \end{pmatrix} \\ &= \begin{pmatrix} rv & 0 \\ 0 & uy \end{pmatrix} \end{aligned}$$

and

$$\begin{aligned} \phi(\mathbf{A})\phi(\mathbf{B}) &= \phi\begin{pmatrix} r & 0 \\ t & u \end{pmatrix}\phi\begin{pmatrix} v & 0 \\ x & y \end{pmatrix} \\ &= \begin{pmatrix} r & 0 \\ 0 & u \end{pmatrix}\begin{pmatrix} v & 0 \\ 0 & y \end{pmatrix} \\ &= \begin{pmatrix} rv & 0 \\ 0 & uy \end{pmatrix}. \end{aligned}$$

Thus $\phi(\mathbf{AB}) = \phi(\mathbf{A})\phi(\mathbf{B})$. Hence ϕ is a homomorphism.

(b) Let $\mathbf{A}, \mathbf{B} \in L$. We have to show that

$$\phi(\mathbf{AB}) = \phi(\mathbf{A})\phi(\mathbf{B}).$$

Now

$$\mathbf{A} = \begin{pmatrix} r & 0 \\ t & u \end{pmatrix} \quad \text{and} \quad \mathbf{B} = \begin{pmatrix} v & 0 \\ x & y \end{pmatrix},$$

for some $r, t, u, v, x, y \in \mathbb{R}$ with $ru \neq 0$ and $vy \neq 0$. Hence

$$\begin{aligned} \phi(\mathbf{AB}) &= \phi\left(\begin{pmatrix} r & 0 \\ t & u \end{pmatrix}\begin{pmatrix} v & 0 \\ x & y \end{pmatrix}\right) \\ &= \phi\begin{pmatrix} rv & 0 \\ tv + ux & uy \end{pmatrix} \\ &= \begin{pmatrix} rv & 0 \\ rv - uy & uy \end{pmatrix} \end{aligned}$$

and

$$\begin{aligned} \phi(\mathbf{A})\phi(\mathbf{B}) &= \phi\begin{pmatrix} r & 0 \\ t & u \end{pmatrix}\phi\begin{pmatrix} v & 0 \\ x & y \end{pmatrix} \\ &= \begin{pmatrix} r & 0 \\ r-u & u \end{pmatrix}\begin{pmatrix} v & 0 \\ v-y & y \end{pmatrix} \\ &= \begin{pmatrix} rv & 0 \\ rv - uv + uv - uy & uy \end{pmatrix} \\ &= \begin{pmatrix} rv & 0 \\ rv - uy & uy \end{pmatrix}. \end{aligned}$$

Thus $\phi(\mathbf{AB}) = \phi(\mathbf{A})\phi(\mathbf{B})$. Hence ϕ is a homomorphism.

Solution to Exercise E110

The homomorphism property for ϕ is

$$\phi(\mathbf{AB}) = \phi(\mathbf{A})\phi(\mathbf{B}) \quad \text{for all } \mathbf{A}, \mathbf{B} \in \mathrm{GL}(2).$$

The mapping ϕ does not have this property. For example, the matrices

$$\mathbf{A} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad \mathbf{B} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$$

are both elements of GL(2) (since they both have determinant 1 and are therefore invertible), and

$$\begin{aligned} \phi(\mathbf{AB}) &= (\mathbf{AB})^{-1} \\ &= \left(\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}\right)^{-1} \\ &= \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}^{-1} \\ &= \begin{pmatrix} 1 & -1 \\ -1 & 2 \end{pmatrix}, \end{aligned}$$

whereas

$$\begin{aligned} \phi(\mathbf{A})\phi(\mathbf{B}) &= \mathbf{A}^{-1}\mathbf{B}^{-1} \\ &= \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^{-1}\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}^{-1} \\ &= \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 2 & -1 \\ -1 & 1 \end{pmatrix}. \end{aligned}$$

Thus $\phi(\mathbf{AB}) \neq \phi(\mathbf{A})\phi(\mathbf{B})$. Hence ϕ is not a homomorphism.

Solution to Exercise E111

(a) The homomorphism property for ϕ is

$$\phi(\mathbf{AB}) = \phi(\mathbf{A}) + \phi(\mathbf{B}) \quad \text{for all } \mathbf{A}, \mathbf{B} \in L.$$

The mapping ϕ does not have this property. For example, the matrix

$$\mathbf{I} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

is an element of L, and

$$\phi(\mathbf{I}\,\mathbf{I}) = \phi(\mathbf{I}) = 1 + 1 = 2,$$

whereas

$$\phi(\mathbf{I}) + \phi(\mathbf{I}) = 1 + 1 + 1 + 1 = 4.$$

Thus $\phi(\mathbf{II}) \neq \phi(\mathbf{I}) + \phi(\mathbf{I})$. Hence ϕ is not a homomorphism.

(b) The homomorphism property for ϕ is

$$\phi(\mathbf{AB}) = \phi(\mathbf{A})\phi(\mathbf{B}) \quad \text{for all } \mathbf{A}, \mathbf{B} \in L.$$

We check whether it holds. Let $\mathbf{A}, \mathbf{B} \in L$. Then

$$\mathbf{A} = \begin{pmatrix} r & 0 \\ t & u \end{pmatrix} \quad \text{and} \quad \mathbf{B} = \begin{pmatrix} v & 0 \\ x & y \end{pmatrix},$$

for some $r, t, u, v, x, y \in \mathbb{R}$ with $ru \neq 0$ and $vy \neq 0$. Hence

$$\begin{aligned} \phi(\mathbf{AB}) &= \phi\left(\begin{pmatrix} r & 0 \\ t & u \end{pmatrix}\begin{pmatrix} v & 0 \\ x & y \end{pmatrix}\right) \\ &= \phi\begin{pmatrix} rv & 0 \\ tv + ux & uy \end{pmatrix} \\ &= (rv)^2(uy)^2 \\ &= (ruvy)^2 \end{aligned}$$

and

$$\begin{aligned} \phi(\mathbf{A})\phi(\mathbf{B}) &= \phi\begin{pmatrix} r & 0 \\ t & u \end{pmatrix}\phi\begin{pmatrix} v & 0 \\ x & y \end{pmatrix} \\ &= r^2u^2v^2y^2 \\ &= (ruvy)^2. \end{aligned}$$

Thus $\phi(\mathbf{AB}) = \phi(\mathbf{A})\phi(\mathbf{B})$. Hence ϕ is a homomorphism.

(c) The homomorphism property for ϕ is

$$\phi(\mathbf{AB}) = \phi(\mathbf{A})\phi(\mathbf{B}) \quad \text{for all } \mathbf{A}, \mathbf{B} \in L.$$

We check whether it holds. Let $\mathbf{A}, \mathbf{B} \in L$. Then

$$\mathbf{A} = \begin{pmatrix} r & 0 \\ t & u \end{pmatrix} \quad \text{and} \quad \mathbf{B} = \begin{pmatrix} v & 0 \\ x & y \end{pmatrix},$$

for some $r, t, u, v, x, y \in \mathbb{R}$ with $ru \neq 0$ and $vy \neq 0$. Hence

$$\begin{aligned} \phi(\mathbf{AB}) &= \phi\left(\begin{pmatrix} r & 0 \\ t & u \end{pmatrix}\begin{pmatrix} v & 0 \\ x & y \end{pmatrix}\right) \\ &= \phi\begin{pmatrix} rv & 0 \\ tv + ux & uy \end{pmatrix} \\ &= \frac{rv}{uy} \end{aligned}$$

and

$$\begin{aligned} \phi(\mathbf{A})\phi(\mathbf{B}) &= \phi\begin{pmatrix} r & 0 \\ t & u \end{pmatrix}\phi\begin{pmatrix} v & 0 \\ x & y \end{pmatrix} \\ &= \frac{r}{u} \times \frac{v}{y} \\ &= \frac{rv}{uy}. \end{aligned}$$

Thus $\phi(\mathbf{AB}) = \phi(\mathbf{A})\phi(\mathbf{B})$. Hence ϕ is a homomorphism.

Solution to Exercise E112

First we prove the 'if' part. Suppose that G is abelian. Then, for all $x, y \in G$,

$$\begin{aligned} \phi(x \circ y) &= (x \circ y) \circ (x \circ y) \\ &= x \circ (y \circ x) \circ y \\ &= x \circ (x \circ y) \circ y \quad \text{(since } G \text{ is abelian)} \\ &= (x \circ x) \circ (y \circ y) \\ &= \phi(x) \circ \phi(y). \end{aligned}$$

Hence ϕ is a homomorphism.

Now we prove the 'only if' part. Suppose that ϕ is a homomorphism. Then, for all $x, y \in G$,

$$\phi(x \circ y) = \phi(x) \circ \phi(y),$$

that is,

$$(x \circ y) \circ (x \circ y) = (x \circ x) \circ (y \circ y).$$

We can write this as

$$x \circ (y \circ x) \circ y = x \circ (x \circ y) \circ y.$$

It now follows by the Cancellation Laws that

$$y \circ x = x \circ y.$$

Hence G is abelian.

Thus ϕ is a homomorphism if and only if G is abelian.

Solution to Exercise E113

Let $x, y, z \in G$. Then

$$\begin{aligned}\phi(x \circ y \circ z) &= \phi((x \circ y) \circ z) \\ &= \phi(x \circ y) * \phi(z) \\ &\quad \text{(by the homomorphism property for } \phi) \\ &= (\phi(x) * \phi(y)) * \phi(z) \\ &\quad \text{(by the homomorphism property for } \phi \text{ again)} \\ &= \phi(x) * \phi(y) * \phi(z),\end{aligned}$$

as required.

Solution to Exercise E114

(a) The identity in both the domain group and the codomain group is 1, and $\phi(1) = 1^2 = 1$.

(b) The identity in both the domain group and the codomain group is 0, and $\phi(0) = 3 \times_6 0 = 0$.

Solution to Exercise E115

(a) In $\mathbb{R}^*$, the inverse of 3 is $\frac{1}{3}$. Now

$$\phi(3) = 9 \quad \text{and} \quad \phi\left(\tfrac{1}{3}\right) = \tfrac{1}{9}.$$

In $\mathbb{R}^*$, the elements 9 and $\frac{1}{9}$ are inverses of each other.

(b) In $\mathbb{Z}_6$, the inverse of 4 is 2. Now

$$\phi(4) = 0 \quad \text{and} \quad \phi(2) = 0.$$

In $\mathbb{Z}_6$, the element 0 is the inverse of 0.

Solution to Exercise E116

(a) In $\mathbb{R}^*$,

$$\phi(3^2) = \phi(9) = 9^2 = 81$$

and

$$(\phi(3))^2 = 9^2 = 81,$$

so $\phi(3^2) = (\phi(3))^2$.

(b) In $\mathbb{Z}_6$,

$$\phi(4 +_6 4) = \phi(2) = 3 \times_6 2 = 0$$

and

$$\begin{aligned}\phi(4) +_6 \phi(4) &= (3 \times_6 4) +_6 (3 \times_6 4) \\ &= 0 +_6 0 = 0,\end{aligned}$$

so $\phi(4 +_6 4) = \phi(4) +_6 \phi(4)$.

Solution to Exercise E117

(a) The image of ϕ_3 is $\{1, 3, 5, 7\} = U_8$, its whole codomain.

(b) The image of ϕ_4 is $\mathbb{R}^+$, again its whole codomain.

Solution to Exercise E118

(a) The homomorphism ϕ maps each integer n to its remainder on division by 12.

It is not one-to-one because, for example, $\phi(1) = \phi(13)$.

However, each element of $\mathbb{Z}_{12}$ occurs as an image under ϕ, so $\operatorname{Im}\phi = \mathbb{Z}_{12}$ and hence ϕ is onto.

(b) The homomorphism ϕ is one-to-one, because if $m, n \in \mathbb{Z}$ and $\phi(m) = \phi(n)$, then $2^m = 2^n$, which gives $m = n$.

The image of ϕ is the set of all integer powers of 2. That is,

$$\operatorname{Im}\phi = \{2^n : n \in \mathbb{Z}\}.$$

There is no integer n such that $2^n = 3$, for example, so ϕ is not onto.

Solution to Exercise E119

(a) The group $(\mathbb{Z}_{12}, +_{12})$ is cyclic so, by Theorem E49, any homomorphism with this group as its domain group must have a cyclic image. This image cannot be $(S(\triangle), \circ)$, because this group is not cyclic.

Alternatively, you may have observed that $\mathbb{Z}_{12}$ is abelian, but $(S(\triangle), \circ)$ is not.

(b) The first argument given in part (a) applies to this case too, because $(S(\square), \circ)$ is not cyclic.

(However, $(S(\square), \circ)$ is abelian, so the second argument does not apply here.)

Solution to Exercise E120

(a) The identity element of the codomain group of ϕ_3 is 1. The kernel of ϕ_3 is $\{e\}$.

(b) The identity element of the codomain group of ϕ_4 is 1. The kernel of ϕ_4 is $\{1, -1\}$.

Solution to Exercise E121

(a) The elements of $\mathbb{Z}_6$ are 0, 1, 2, 3, 4 and 5, and 0 is the identity element. We have

$$\begin{aligned}\phi(0) &= 0,\\ \phi(1) &= 3,\\ \phi(2) &= 0,\\ \phi(3) &= 3,\\ \phi(4) &= 0,\\ \phi(5) &= 3.\end{aligned}$$

Hence $\operatorname{Im}\phi = \{0, 3\}$ and $\operatorname{Ker}\phi = \{0, 2, 4\}$.

(b) This homomorphism ϕ, the exponential function, has image $(0, \infty) = \mathbb{R}^+$ (as you saw in Subsection 4.2 of Unit D4). That is,

$$\operatorname{Im}\phi = \mathbb{R}^+.$$

(So ϕ is onto.)

Also, ϕ is one-to-one (since it is strictly increasing, as you saw in Subsection 4.2 of Unit D4). Hence, since the identity element in the domain group is 0,

$$\operatorname{Ker}\phi = \{0\},$$

by Theorem E52.

(c) This is the trivial homomorphism from $(\mathbb{R}^*, \times)$ to $(\mathbb{R}^*, \times)$. Every element of the domain group is mapped by ϕ to the identity element 1 of the codomain group. Therefore

$$\operatorname{Im}\phi = \{1\}$$

and $\operatorname{Ker}\phi$ is the whole domain group, that is,

$$\operatorname{Ker}\phi = \mathbb{R}^*.$$

Solution to Exercise E122

First we show that ϕ is a homomorphism. Let $m, n \in \mathbb{Z}$. We have to show that

$$\phi(m + n) = \phi(m) + \phi(n).$$

Now

$$\begin{aligned}\phi(m + n) &= 7(m + n)\\ &= 7m + 7n\\ &= \phi(m) + \phi(n).\end{aligned}$$

Hence ϕ is a homomorphism.

Now we find the image of ϕ. It is

$$\begin{aligned}\operatorname{Im}\phi &= \{\phi(n) : n \in \mathbb{Z}\}\\ &= \{7n : n \in \mathbb{Z}\}\\ &= 7\mathbb{Z}\\ &= \{\ldots, -14, -7, 0, 7, 14, \ldots\}.\end{aligned}$$

(The final line above could be omitted.)

Finally we find the kernel of ϕ. The identity element of the codomain group is 0. So the kernel is

$$\begin{aligned}\operatorname{Ker}\phi &= \{n \in \mathbb{Z} : \phi(n) = 0\}\\ &= \{n \in \mathbb{Z} : 7n = 0\}\\ &= \{n \in \mathbb{Z} : n = 0\}\\ &= \{0\}.\end{aligned}$$

(Alternatively, we can find the kernel by showing that ϕ is one-to-one and applying Theorem E52.)

Solution to Exercise E123

We have

$$\begin{aligned}\operatorname{Im}\phi &= \left\{\phi\begin{pmatrix}a & 0\\ c & d\end{pmatrix} : \begin{pmatrix}a & 0\\ c & d\end{pmatrix} \in L\right\}\\ &= \left\{\begin{pmatrix}1 & 0\\ 0 & d^2\end{pmatrix} : d \in \mathbb{R},\ d \neq 0\right\}\\ &= \left\{\begin{pmatrix}1 & 0\\ 0 & r\end{pmatrix} : r \in \mathbb{R}^+\right\}.\end{aligned}$$

(Here we have used the fact that, as d runs through all non-zero values in $\mathbb{R}$, its square d^2 takes all *positive* values in $\mathbb{R}$, so we can specify the set $\operatorname{Im}\phi$ equally well by replacing d^2 with r, say, where $r \in \mathbb{R}^+$.)

The identity element of the codomain group $(L, \times)$ is $\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}$, so

$$\operatorname{Ker}\phi = \left\{\begin{pmatrix}a & 0\\ c & d\end{pmatrix} \in L : \phi\begin{pmatrix}a & 0\\ c & d\end{pmatrix} = \begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}\right\}.$$

Now

$$\begin{aligned}\phi\begin{pmatrix}a & 0\\ c & d\end{pmatrix} = \begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix} &\iff \begin{pmatrix}1 & 0\\ 0 & d^2\end{pmatrix} = \begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}\\ &\iff d^2 = 1\\ &\iff d = \pm 1.\end{aligned}$$

Thus

$$\begin{aligned}\operatorname{Ker}\phi &= \left\{\begin{pmatrix} a & 0 \\ c & d \end{pmatrix} \in L : d = \pm 1\right\} \\ &= \left\{\begin{pmatrix} a & 0 \\ c & d \end{pmatrix} : a, c, d \in \mathbb{R},\ ad \neq 0,\ d = \pm 1\right\} \\ &= \left\{\begin{pmatrix} a & 0 \\ c & \pm 1 \end{pmatrix} : a, c \in \mathbb{R},\ a \neq 0\right\}.\end{aligned}$$

Solution to Exercise E124

The identity element of the codomain group $(D, \times)$ is the identity matrix $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, so

$$\begin{aligned}\operatorname{Ker}\phi &= \left\{\begin{pmatrix} a & 0 \\ c & d \end{pmatrix} \in L : \phi\begin{pmatrix} a & 0 \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\right\} \\ &= \left\{\begin{pmatrix} a & 0 \\ c & d \end{pmatrix} \in L : \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\right\} \\ &= \left\{\begin{pmatrix} a & 0 \\ c & d \end{pmatrix} \in L : a = d = 1\right\} \\ &= \left\{\begin{pmatrix} a & 0 \\ c & d \end{pmatrix} : a, c, d \in \mathbb{R},\ ad \neq 0,\ a = d = 1\right\} \\ &= \left\{\begin{pmatrix} 1 & 0 \\ c & 1 \end{pmatrix} : c \in \mathbb{R}\right\}.\end{aligned}$$

Solution to Exercise E125

Let r be an element of the codomain group $(\mathbb{R}^*, \times)$. Then the matrix

$$\begin{pmatrix} r & 0 \\ 0 & 1 \end{pmatrix}$$

is an element of the domain group $(L, \times)$, because it is lower triangular and its determinant is $r \times 1 = r$ which is non-zero because $r \in \mathbb{R}^*$, and

$$\phi\begin{pmatrix} r & 0 \\ 0 & 1 \end{pmatrix} = r.$$

Thus ϕ is onto and therefore $\operatorname{Im}\phi = \mathbb{R}^*$.

Solution to Exercise E126

First we show that $\operatorname{Im}\phi \subseteq \mathbb{R}^+$. Let $r \in \operatorname{Im}\phi$. Then

$$r = \phi(x)$$

for some element x of $\mathbb{R}^*$. This gives

$$r = x^2.$$

Since $x \in \mathbb{R}^*$, it follows that $r > 0$ and hence $r \in \mathbb{R}^+$. Therefore $\operatorname{Im}\phi \subseteq \mathbb{R}^+$.

Now we show that $\mathbb{R}^+ \subseteq \operatorname{Im}\phi$. Let $r \in \mathbb{R}^+$. Then r is the image under ϕ of the real number $\sqrt{r}$, since

$$\phi\left(\sqrt{r}\right) = \left(\sqrt{r}\right)^2 = r.$$

Hence $r \in \operatorname{Im}\phi$. Therefore $\mathbb{R}^+ \subseteq \operatorname{Im}\phi$.

Since $\operatorname{Im}\phi \subseteq \mathbb{R}^+$ and $\mathbb{R}^+ \subseteq \operatorname{Im}\phi$, it follows that $\operatorname{Im}\phi = \mathbb{R}^+$.

Solution to Exercise E127

(a) The mapping ϕ is a homomorphism because, for any $m, n \in \mathbb{Z}_{12}$,

$$\begin{aligned}\phi(m +_{12} n) &= 2 \times_{12} (m +_{12} n) \\ &= (2 \times_{12} m) +_{12} (2 \times_{12} n) \\ &= \phi(m) +_{12} \phi(n).\end{aligned}$$

(b) The identity element of the codomain group is 0, so

$$\begin{aligned}\operatorname{Ker}\phi &= \{n \in \mathbb{Z}_{12} : \phi(n) = 0\} \\ &= \{n \in \mathbb{Z}_{12} : 2 \times_{12} n = 0\} \\ &= \{0, 6\}.\end{aligned}$$

The cosets of $\operatorname{Ker}\phi$ are

$$\begin{aligned}\operatorname{Ker}\phi &= \{0, 6\}, \\ 1 + \operatorname{Ker}\phi &= \{1, 7\}, \\ 2 + \operatorname{Ker}\phi &= \{2, 8\}, \\ 3 + \operatorname{Ker}\phi &= \{3, 9\}, \\ 4 + \operatorname{Ker}\phi &= \{4, 10\}, \\ 5 + \operatorname{Ker}\phi &= \{5, 11\}.\end{aligned}$$

(c) We have

$$\begin{aligned}\phi(0) &= \phi(6) = 0, \\ \phi(1) &= \phi(7) = 2, \\ \phi(2) &= \phi(8) = 4, \\ \phi(3) &= \phi(9) = 6, \\ \phi(4) &= \phi(10) = 8, \\ \phi(5) &= \phi(11) = 10.\end{aligned}$$

Thus the partition of $\mathbb{Z}_{12}$ obtained by collecting together elements of $\mathbb{Z}_{12}$ with the same image is

$$\{0, 6\}, \quad \{1, 7\}, \quad \{2, 8\}, \quad \{3, 9\}, \quad \{4, 10\}, \quad \{5, 11\}.$$

As expected this is the same as the partition of $\mathbb{Z}_{12}$ into cosets of $\operatorname{Ker}\phi$ found in part (b).

Solution to Exercise E128

(a) The kernel of ϕ is the set of integers that ϕ maps to 0, so

$$\operatorname{Ker}\phi = \{5n : n \in \mathbb{Z}\} = 5\mathbb{Z}.$$

The cosets of $\operatorname{Ker}\phi$ are

$$\begin{aligned}
5\mathbb{Z} &= \{5n : n \in \mathbb{Z}\},\\
1 + 5\mathbb{Z} &= \{5n + 1 : n \in \mathbb{Z}\},\\
2 + 5\mathbb{Z} &= \{5n + 2 : n \in \mathbb{Z}\},\\
3 + 5\mathbb{Z} &= \{5n + 3 : n \in \mathbb{Z}\},\\
4 + 5\mathbb{Z} &= \{5n + 4 : n \in \mathbb{Z}\}.
\end{aligned}$$

(b) The set of integers with a particular image, say s, under ϕ is the set of integers whose remainder on division by 5 is s. Thus the partition obtained by collecting together integers with the same image consists of the five sets listed in part (a), as expected.

Solution to Exercise E129

(a) The mapping ϕ is a linear transformation, because it is of the form

$$(x, y) \longmapsto ax + by$$

where $a, b \in \mathbb{R}$. Hence, by Proposition E39, it is a homomorphism.

(Alternatively, we can show that ϕ is a homomorphism as follows.

Let $(x_1, y_1), (x_2, y_2) \in \mathbb{R}^2$. We have to show that

$$\phi((x_1, y_1) + (x_2, y_2)) = \phi(x_1, y_1) + \phi(x_2, y_2).$$

Now

$$\begin{aligned}
\phi((x_1, y_1) + (x_2, y_2)) &= \phi(x_1 + x_2, y_1 + y_2)\\
&= (x_1 + x_2) + (y_1 + y_2)\\
&= (x_1 + y_1) + (x_2 + y_2)\\
&= \phi(x_1, y_1) + \phi(x_2, y_2).
\end{aligned}$$

Hence ϕ is a homomorphism.)

(b) The homomorphism ϕ is onto, since if x is an element of the codomain group $(\mathbb{R}, +)$ then x is the image under ϕ of the element $(x, 0)$ of the domain group $(\mathbb{R}^2, +)$, because

$$\phi(x, 0) = x + 0 = x.$$

Hence

$$\operatorname{Im}\phi = \mathbb{R}.$$

Also

$$\begin{aligned}
\operatorname{Ker}\phi &= \{(x, y) \in \mathbb{R}^2 : \phi(x, y) = 0\}\\
&= \{(x, y) \in \mathbb{R}^2 : x + y = 0\}\\
&= \{(x, y) \in \mathbb{R}^2 : y = -x\}.
\end{aligned}$$

(This is the line $y = -x$ in $\mathbb{R}^2$, that is, the line through the origin with gradient -1.)

(Alternatively we can write $\operatorname{Ker}\phi$ as

$$\operatorname{Ker}\phi = \{(k, -k) : k \in \mathbb{R}\}.)$$

(c) By the First Isomorphism Theorem,

$$\mathbb{R}^2/\operatorname{Ker}\phi \cong \operatorname{Im}\phi,$$

so

$$\mathbb{R}^2/\operatorname{Ker}\phi \cong (\mathbb{R}, +).$$

So a standard group isomorphic to $\mathbb{R}^2/\operatorname{Ker}\phi$ is $(\mathbb{R}, +)$.

Solution to Exercise E130

(a) Let $\mathbf{A}, \mathbf{B} \in L$. We have to show that

$$\phi(\mathbf{AB}) = \phi(\mathbf{A})\phi(\mathbf{B}).$$

Now

$$\mathbf{A} = \begin{pmatrix} r & 0 \\ t & u \end{pmatrix} \quad \text{and} \quad \mathbf{B} = \begin{pmatrix} v & 0 \\ x & y \end{pmatrix},$$

for some $r, t, u, v, x, y \in \mathbb{R}$, where $ru \neq 0$ and $vy \neq 0$. Hence

$$\begin{aligned}
\phi(\mathbf{AB}) &= \phi\left(\begin{pmatrix} r & 0 \\ t & u \end{pmatrix}\begin{pmatrix} v & 0 \\ x & y \end{pmatrix}\right)\\
&= \phi\begin{pmatrix} rv & 0 \\ tv + ux & uy \end{pmatrix}\\
&= rvuy\\
&= ruvy
\end{aligned}$$

and

$$\begin{aligned}
\phi(\mathbf{A})\phi(\mathbf{B}) &= \phi\begin{pmatrix} r & 0 \\ t & u \end{pmatrix}\phi\begin{pmatrix} v & 0 \\ x & y \end{pmatrix}\\
&= ruvy.
\end{aligned}$$

Thus $\phi(\mathbf{AB}) = \phi(\mathbf{A})\phi(\mathbf{B})$. Hence ϕ is a homomorphism.

(b) The homomorphism ϕ is onto, because if $r \in \mathbb{R}^*$ then r is the image under ϕ of the matrix

$$\begin{pmatrix} r & 0 \\ 0 & 1 \end{pmatrix}.$$

This matrix is in L because it is lower triangular and its determinant is $r \times 1 = r$, which is non-zero because $r \in \mathbb{R}^*$. Hence

$$\operatorname{Im}\phi = \mathbb{R}^*.$$

The identity element of the codomain group is 1, so

$$\begin{aligned}
\operatorname{Ker}\phi &= \left\{ \begin{pmatrix} a & 0 \\ c & d \end{pmatrix} \in L : \phi \begin{pmatrix} a & 0 \\ c & d \end{pmatrix} = 1 \right\} \\
&= \left\{ \begin{pmatrix} a & 0 \\ c & d \end{pmatrix} \in L : ad = 1 \right\} \\
&= \left\{ \begin{pmatrix} a & 0 \\ c & d \end{pmatrix} \in L : d = 1/a \right\} \\
&= \left\{ \begin{pmatrix} a & 0 \\ c & 1/a \end{pmatrix} : a, c \in \mathbb{R},\ a \neq 0 \right\}.
\end{aligned}$$

(c) By the First Isomorphism Theorem,

$$L/\operatorname{Ker}\phi \cong (\mathbb{R}^*, \times).$$

So a standard group isomorphic to $L/\operatorname{Ker}\phi$ is $(\mathbb{R}^*, \times)$.

Solution to Exercise E131

(a) Let $\mathbf{A}, \mathbf{B} \in L$. We have to show that

$$\phi(\mathbf{AB}) = \phi(\mathbf{A})\phi(\mathbf{B}).$$

Now

$$\mathbf{A} = \begin{pmatrix} r & 0 \\ t & u \end{pmatrix} \quad \text{and} \quad \mathbf{B} = \begin{pmatrix} v & 0 \\ x & y \end{pmatrix},$$

for some $r, t, u, v, x, y \in \mathbb{R}$ with $ru \neq 0$ and $vy \neq 0$. Hence

$$\begin{aligned}
\phi(\mathbf{AB}) &= \phi\left(\begin{pmatrix} r & 0 \\ t & u \end{pmatrix} \begin{pmatrix} v & 0 \\ x & y \end{pmatrix} \right) \\
&= \phi \begin{pmatrix} rv & 0 \\ tv + ux & uy \end{pmatrix} \\
&= \begin{pmatrix} 1/(rv) & 0 \\ 0 & 1 \end{pmatrix}
\end{aligned}$$

and

$$\begin{aligned}
\phi(\mathbf{A})\phi(\mathbf{B}) &= \phi \begin{pmatrix} r & 0 \\ t & u \end{pmatrix} \phi \begin{pmatrix} v & 0 \\ x & y \end{pmatrix} \\
&= \begin{pmatrix} 1/r & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1/v & 0 \\ 0 & 1 \end{pmatrix} \\
&= \begin{pmatrix} 1/(rv) & 0 \\ 0 & 1 \end{pmatrix}.
\end{aligned}$$

Thus $\phi(\mathbf{AB}) = \phi(\mathbf{A})\phi(\mathbf{B})$. Hence ϕ is a homomorphism.

(b) We have

$$\begin{aligned}
\operatorname{Im}\phi &= \left\{ \phi \begin{pmatrix} a & 0 \\ c & d \end{pmatrix} : \begin{pmatrix} a & 0 \\ c & d \end{pmatrix} \in L \right\} \\
&= \left\{ \begin{pmatrix} 1/a & 0 \\ 0 & 1 \end{pmatrix} : a \in \mathbb{R}^* \right\} \\
&= \left\{ \begin{pmatrix} r & 0 \\ 0 & 1 \end{pmatrix} : r \in \mathbb{R}^* \right\}.
\end{aligned}$$

The identity element of the codomain group is

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$

so

$$\begin{aligned}
\operatorname{Ker}\phi &= \left\{ \begin{pmatrix} a & 0 \\ c & d \end{pmatrix} \in L : \phi \begin{pmatrix} a & 0 \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right\} \\
&= \left\{ \begin{pmatrix} a & 0 \\ c & d \end{pmatrix} \in L : \begin{pmatrix} 1/a & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right\} \\
&= \left\{ \begin{pmatrix} a & 0 \\ c & d \end{pmatrix} \in L : 1/a = 1 \right\} \\
&= \left\{ \begin{pmatrix} a & 0 \\ c & d \end{pmatrix} \in L : a = 1 \right\} \\
&= \left\{ \begin{pmatrix} 1 & 0 \\ c & d \end{pmatrix} : c, d \in \mathbb{R},\ d \neq 0 \right\}.
\end{aligned}$$

(c) By the First Isomorphism Theorem, the quotient group $L/\operatorname{Ker}\phi$ is isomorphic to $\operatorname{Im}\phi$.

We now show that $\operatorname{Im}\phi$ is isomorphic to $(\mathbb{R}^*, \times)$. Consider the mapping

$$\begin{aligned}
\theta : \operatorname{Im}\phi &\longrightarrow \mathbb{R}^* \\
\begin{pmatrix} r & 0 \\ 0 & 1 \end{pmatrix} &\longmapsto r.
\end{aligned}$$

This mapping is one-to-one, because if

$$\mathbf{A} = \begin{pmatrix} r & 0 \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad \mathbf{B} = \begin{pmatrix} s & 0 \\ 0 & 1 \end{pmatrix}$$

are elements of $\operatorname{Im}\phi$ such that $\theta(\mathbf{A}) = \theta(\mathbf{B})$, then $r = s$ by the definition of θ and hence $\mathbf{A} = \mathbf{B}$.

It is also onto, because if $r \in \mathbb{R}^*$ then r is the image under θ of the element

$$\begin{pmatrix} r & 0 \\ 0 & 1 \end{pmatrix}$$

of $\operatorname{Im}\phi$.

Finally, it has the homomorphism property because, for all $r, s \in \mathbb{R}^*$,

$$\begin{aligned} \theta\left(\begin{pmatrix} r & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} s & 0 \\ 0 & 1 \end{pmatrix}\right) &= \theta\begin{pmatrix} rs & 0 \\ 0 & 1 \end{pmatrix} \\ &= rs \\ &= \theta\begin{pmatrix} r & 0 \\ 0 & 1 \end{pmatrix}\theta\begin{pmatrix} s & 0 \\ 0 & 1 \end{pmatrix}. \end{aligned}$$

Thus θ is an isomorphism, so

$$L/\operatorname{Ker}\phi \cong \operatorname{Im}\phi \cong (\mathbb{R}^*, \times).$$

Solution to Exercise E132

(a) Let $\phi : \mathbb{Z}_{11} \longrightarrow S_3$ be a homomorphism. By Corollary E56 and Lagrange's Theorem, the order of $\operatorname{Im}\phi$ divides the orders of $\mathbb{Z}_{11}$ and S_3, which are 11 and 6, respectively. But 11 and 6 have greatest common factor 1, so the order of $\operatorname{Im}\phi$ is 1. Hence, since $\operatorname{Im}\phi$ is a subgroup of S_3, we have $\operatorname{Im}\phi = \{e\}$. Therefore ϕ is the trivial homomorphism

$$\begin{aligned} \phi : \mathbb{Z}_{11} &\longrightarrow S_3 \\ n &\longmapsto e. \end{aligned}$$

(b) Let $\phi : S(\triangle) \longrightarrow \mathbb{Z}_3$ be a homomorphism. By Corollary E56 and Lagrange's Theorem, the order of $\operatorname{Im}\phi$ divides the orders of $S(\triangle)$ and $\mathbb{Z}_3$, which are 6 and 3, respectively. Hence the order of $\operatorname{Im}\phi$ is either 1 or 3.

If $\operatorname{Im}\phi$ has order 3, then $\operatorname{Ker}\phi$ has order 2, by Corollary E56. As $S(\triangle)$ does not have a normal subgroup of order 2 (by the solution to Exercise E39 in Subsection 3.3 of Unit E2), this is impossible.

Thus $\operatorname{Im}\phi$ has order 1. Hence, since $\operatorname{Im}\phi$ is a subgroup of $(\mathbb{Z}_3, +_3)$, we have $\operatorname{Im}\phi = \{0\}$. Therefore ϕ is the trivial homomorphism

$$\begin{aligned} \phi : S(\triangle) &\longrightarrow \mathbb{Z}_3 \\ f &\longmapsto 0. \end{aligned}$$

Solution to Exercise E133

(a) We have

$$\begin{aligned} &(2,3) + \operatorname{Ker}\phi \\ &= \{(2+x, 3+y) : (x,y) \in \mathbb{R}^2,\ y = -x\} \\ &= \{(x,y) : (x-2, y-3) \in \mathbb{R}^2,\ y - 3 = -(x-2)\} \\ &= \{(x,y) : (x,y) \in \mathbb{R}^2,\ y = -x + 5\} \\ &= \{(x,y) \in \mathbb{R}^2 :\ y = -x + 5\}. \end{aligned}$$

This is the line $y = -x + 5$, that is, the line with gradient -1 and y-intercept 5.

(Alternatively we can find $(2,3) + \operatorname{Ker}\phi$ as follows.

$$\begin{aligned} (2,3) + \operatorname{Ker}\phi &= \{(2+k, 3-k) : k \in \mathbb{R}\} \\ &= \{(k, 3-(k-2)) : k - 2 \in \mathbb{R}\} \\ &= \{(k, -k+5) : k \in \mathbb{R}\}. \end{aligned}$$

This is the line $y = -x + 5$.)

(A third way to find the coset $(2,3) + \operatorname{Ker}\phi$ is as follows. Since $\operatorname{Ker}\phi$ is the line $y = -x$, the coset $(2,3) + \operatorname{Ker}\phi$ is the line obtained by translating the line $y = -x$ by two units to the right and three units up. Since the line $y = -x$ has gradient -1, translating it by two units to the right increases its y-intercept by 2 units, and then translating it by three units up increases its y-intercept by another 3 units. Its gradient remains unchanged throughout, so we obtain the line $y = -x + 5$.)

(b) Similarly,

$$\begin{aligned} &(a,b) + \operatorname{Ker}\phi \\ &= \{(a+x, b+y) : (x,y) \in \mathbb{R}^2,\ y = -x\} \\ &= \{(x,y) : (x-a, y-b) \in \mathbb{R}^2,\ y - b = -(x-a)\} \\ &= \{(x,y) : (x,y) \in \mathbb{R}^2,\ y = -x + (a+b)\} \\ &= \{(x,y) \in \mathbb{R}^2 : y = -x + (a+b)\}. \end{aligned}$$

This is the line $y = -x + (a+b)$, that is, the line with gradient -1 and y-intercept $a+b$.

(Alternatively we can find $(a, b) + \operatorname{Ker}\phi$ as follows.

$$\begin{aligned}(a, b) + \operatorname{Ker}\phi &= \{(a + k, b - k) : k \in \mathbb{R}\} \\ &= \{(k, b - (k - a)) : k - a \in \mathbb{R}\} \\ &= \{(k, -k + (a + b)) : k \in \mathbb{R}\}.\end{aligned}$$

This is the line $y = -x + (a + b)$.)

(A third way to find the coset $(a, b) + \operatorname{Ker}\phi$ is as follows. Since $\operatorname{Ker}\phi$ is the line $y = -x$, the coset $(a, b) + \operatorname{Ker}\phi$ is the line obtained by translating the line $y = -x$ by a units to the right and b units up (if a is negative then the translation by a units to the right is actually a translation to the left, and similarly if b is negative then the translation by b units up is actually a translation down). Since the line $y = -x$ has gradient -1, translating it by a units to the right adds a units to its y-intercept, and then translating it by b units up adds another b units to its y-intercept. Its gradient remains unchanged throughout, so we obtain the line $y = -x + (a + b)$.)

(c) By part (b), each coset of $\operatorname{Ker}\phi$ is a line of the form

$$y = -x + c,$$

where $c \in \mathbb{R}$. Moreover, each such line is a coset of $\operatorname{Ker}\phi$ because, for any $c \in \mathbb{R}$, the line $y = -x + c$ is the coset

$$(0, c) + \operatorname{Ker}\phi.$$

Thus the elements of the quotient group $\mathbb{R}^2/\operatorname{Ker}\phi$ are the lines with gradient -1.

(Some of these elements are shown below.)